SUPERINTENDENCIA
DE BANCOS
REPÚBLICA DOMINICANA

ADQUISICIÓN DE PLATAFORMA DE CORE FIREWALLS CHECKPOINT PARA USO DE LA SUPERINTENDENCIA DE BANCOS

INFORME JUSTIFICATIVO DE MARCA

AGOSTO 2022

Contenido

1. Antecedentes 2

2. Alcance e importancia 2

4. CRITERIOS DE EXCLUSIVIDAD DE LA TECNOLOGIA O SERVICIO 3

5. CONCLUSION: 4

1. Antecedentes

Los ataques a una red son inevitables, y toda red debe ser capaz de resistir una intrusión. Una brecha en la red es un riesgo inevitable en línea. Hay un mecanismo de ciberseguridad que resulta eficaz a la hora de limitar los daños en caso de una brecha en la red. Esta técnica de ciberseguridad es la segmentación de la red, la cual es la práctica de dividir una red informática más grande en varias pequeñas subredes aisladas entre sí. La segmentación de la red puede proteger partes vitales de la red en caso de que se produzcan violaciones de datos. Si el sistema se ve comprometido, este mecanismo de defensa limita los daños que pueden causar los intrusos.

Un componente esencial para la implementación de la segmentación de la red es el core firewall, ya que este nos permite dividir la red de la SB en diferentes subredes y a la vez aplicar las directivas y lineamientos de seguridad establecidos en el Plan de Ciberseguridad del Departamento de Seguridad de la Información.

Tras estudiar las ofertas de productos y características de compañías que proveen firewalls de nueva generación en la República Dominicana, entendemos que la marca Checkpoint y sus productos de Next Generation Firewall (NGFW), es la solución ideal tomando en cuenta su tiempo en el mercado ofreciendo NGFW, que cuentan con un equipo de personas con experticia reconocida en el área de Desarrollo e Investigaciones de Amenazas, así como un conjunto de funcionalidades en sus appliances, que entendemos son las que mejores se alinean con el Plan de Ciberseguridad establecido por el Departamento Seguridad de la Información.

2. Alcance e importancia

La segmentación de red es uno de los mecanismos de seguridad utilizados dentro de la Arquitectura de Zero Trust, la cual el Departamento de Seguridad de la Información tiene planificada implementar en la red de la SB, acorde con los lineamientos del Programa de Ciberseguridad de la SB, y a la vez en cumplimiento con el Reglamento de Seguridad Cibernética y de Información del Banco Central, así como con las mejores prácticas del sector de Seguridad de la Información.

Mediante la implementación de los core firewalls mejorará la postura de seguridad de la SB, permitiendo segmentar la red, creando microperímetros alrededor de los datos, aplicaciones, activos y sistemas más importantes. Esta línea de defensa elimina la capacidad de un atacante para moverse lateralmente a través de una red.

3. ESPECIFICACIONES Y CARACTERISTICAS DEL PRODUCTO REQUERIDO

El TDR de la Adquisición de Plataforma de CORE FIREWALLS de la empresa Checkpoint se encuentra en otro documento que será entregado junto con este informe.

4. CRITERIOS DE EXCLUSIVIDAD DE LA TECNOLOGIA O SERVICIO

El criterio de exclusividad del Next Generation Firewall de Checkpoint viene dado por los siguientes aspectos:

- Mejoramiento del desempeño o performance de los equipos con nuevas versiones del software. Esto implica una arquitectura flexible para el manejo de nuevo tráfico o protocolos de red, en un entorno cambiante como el de la SB, que permite la optimización de los recursos de los firewalls mediante la instalación de nuevas versiones de software, realizando una mejor integración y aumentando su eficiencia.
- Control de Aplicaciones: Aunque esta funcionalidad es ofrecida por los NGFW de varias compañías (Fortinet, Palo Alto, Cisco, etc.), el producto de Checkpoint ofrece una mayor visibilidad de las aplicaciones de alto riesgo y Shadow-IT, pudiendo identificar más de 8,600 aplicaciones. Esta cantidad es mayor que las que tienen publicadas las marcas que compiten con Checkpoint.
- Plataforma robusta y madura: El tener una menor cantidad de vulnerabilidades que las demás marcas de NGFW en el período de tiempo especificado, es una muestra de la madurez y lo robusta que es la plataforma de Checkpoint, en comparación con las demás plataformas.
    - Checkpoint: 52 vulnerabilidades desde 2016 hasta 2021
    - Fortinet: 372 vulnerabilidades desde 2016 hasta 2021
    - Palo Alto: 251 vulnerabilidades desde 2016 hasta 2021
    - Cisco: 390 vulnerabilidades desde 2016 hasta 2021
- Utilización del marco de MITRE ATT&CK: Los NGFW de Checkpoint utilizan el marco de MITRE ATT&CK para prevenir ciberataques, identificando las amenazas, así como las tácticas, técnicas y procedimientos (TTPs) utilizados por esas amenazas. En la SB, el Departamento de Seguridad de la Información está implementando el marco de MITRE

ATT&CK, por lo que los NGFW de Checkpoint se alinean con los objetivos y procesos de ciberseguridad de la SB. Es importante destacar que MITRE es una organización sin fines de lucro y ofrece el marco de MITRE ATT&CK de manera gratuita a todas las organizaciones e individuos que estén interasados para que lo incluyan en sus productos, ya sean Firewalls, Antivirus, EDR, etc. Sin embargo, hasta el día de hoy, no hemos visto que este marco se haya incluido en los NGFW de las demás marcas.

- Cuadrante Líder de Gartner: Los NGFW de Checkpoint han sido nombrados 22 veces consecutivas en el Cuadrante Líder del Cuadrante Mágico de Gartner para Enterprise Network Firewalls. Esto es una muestra de que Checkpoint se ha mantenido innovando y siendo relevante en el mercado de NGFW.

5. CONCLUSION:

Por las razones antes expuestas, se cataloga la adquisición de este producto de NGFW de Checkpoint como un Caso de Excepción, por ser la solución que entendemos que mejor cumple y se alinea al Plan de Ciberseguridad de la SB, además de ser una empresa con una vasta experiencia en el mercado de los NGFW, que se ha mantenido entre los líderes en este mercado innovando y satisfaciendo las necesidades de los equipos de seguridad de las diferentes empresas.

Atentamente,

Eduard Encarnación

Especialista Senior de Seguridad de la Información