TÉRMINOS DE REFERENCIA

ADQUISICION DE PLATAFORMA DE CORE FIREWALLS CHECKPOINT PARA LA SUPERINTENDENCIA DE BANCOS.

1. PLANTEAMIENTO DE LA NECESIDAD

La Superintendencia de Bancos (SB) tiene como parte de su estrategia de ciberseguridad la implementación del modelo de arquitectura Zero Trust. Un control de seguridad esencial dentro de este modelo es la segmentación de la red para evitar y prevenir el movimiento lateral de ataques o accesos no autorizados dentro del ambiente de la SB. Las políticas de segmentación de la red van a ser definidas a través de equipos de Core Firewalls, descritos en este documento para su adquisición.

2. OBJETIVOS

2.1. Objetivo General

Adquirir 4 appliances CheckPoint de Core Firewall en HA (2 para sede y 2 para site alterno) para implementar la segmentación de la red interna de la Superintendencia de Bancos (SB) y las políticas de seguridad correspondientes como parte de la estrategia de ciberseguridad de implementación del modelo de Zero Trust.

Descripción	Cantidad
Core Firewalls Sede	2
Core Firewalls Sitio alterno	2

2.2. Objetivos específicos

- Integración en modelo de Zero Trust de la Superintendencia de Bancos.
- Prevención del movimiento lateral en la red interna de la SB.
- Control de acceso a los servidores de aplicaciones y sistemas

3. Especificaciones de Plataforma de Core Firewalls

- El desempeño o performance de los equipos puede ser mejorado con nuevas versiones del software.
- Los equipos deben contar mínimo con 4 puertos de 10 Gb SFP+ por appliance, así como los transceivers y patch cords para realizar las conexiones a los switches.
- Debe ser NGFW de 3.6 Gbps o más, así como soportar 4 millones de sesiones concurrentes o más.
- Los equipos deben tener disco duro integrado.
- La solución debe proveer protección a Office 365 mediante APIs y mediante modificación de records MX para cualquier otra solución de correo.
- Los firewalls deben ofrecer balanceo de líneas automático.
- Los firewalls deben ofrecer routing dinámico.
- Los firewalls deben estar como líder del cuadrante mágico de Gartner para Enterprise Firewalls.
- La propuesta de la solución debe incluir el entrenamiento oficial del fabricante para 4 personas, impartido por un personal autorizado por fábrica.
- La propuesta de la solución debe incluir soporte del producto 24x7 por parte de fábrica.
- La propuesta de la solución debe incluir soporte del producto 24x7 a nivel local.

Los tipos de capacidades de seguridad de la red que deben ofrecer los firewalls son:

Segmentación de la red: Definir los límites entre los segmentos de la red cuando los activos dentro del grupo tienen una función, riesgo o papel común dentro de la SB, para evitar las amenazas potenciales fuera de cada segmento, proporcionando una mayor seguridad y control de acceso a los datos sensibles de la SB.

Control de acceso: Definir las personas o grupos y los dispositivos que tienen acceso a las aplicaciones y sistemas, negando así el acceso no autorizado, y las amenazas. Permitir integraciones con productos de gestión de identidades y accesos (IAM) para poder identificar claramente al usuario y las políticas de control de acceso basado en roles (RBAC) y así garantizar que la persona y el dispositivo tienen acceso autorizado al activo.

Redes Zero Trust: Los firewalls deben integrarse con el modelo de Zero Trust, dando prioridad a los datos para lograr la seguridad mediante la microsegmentación, aplicando una política de acceso con mínimos privilegios a nivel de red.

Sistemas de prevención de intrusiones (IPS): Los firewalls deben ofrecer la capacidad de detectar o prevenir los ataques a la seguridad de la red, como los ataques de fuerza bruta, los ataques de denegación de servicio (DoS) y la explotación de vulnerabilidades conocidas y de día cero.

Sandboxing: Los firewalls deben poder ejecutar código o abrir archivos en un entorno seguro y aislado en una máquina anfitriona que imita los entornos operativos del usuario final, para observar los archivos o el código a medida que se abren y buscar comportamientos maliciosos para evitar que las amenazas entren en la red.

Seguridad de red a hiperescala: Deben ofrecer capacidad de una arquitectura para escalar adecuadamente, a medida que se añade una mayor demanda al sistema. La solución debe incluir un despliegue rápido y un aumento o disminución de la escala para satisfacer los cambios en las demandas de seguridad de la red. Al integrar estrechamente los recursos de red y computación en un sistema definido por software, es posible utilizar plenamente todos los recursos de hardware disponibles en una solución de clustering.

Seguridad de la red en la nube: Las soluciones de redes definidas por software (SDN) y redes de área amplia definidas por software (SD-WAN) permiten soluciones de seguridad de red en despliegues privados, públicos híbridos y alojados en la nube de Firewall-as-a-Service (FWaaS).

3.1. GESTIÓN DE LA SEGURIDAD

La gestión de la seguridad debe contemplar todo el paradigma operativo de la seguridad:

- Facilidad de uso, donde la interfaz de usuario reduce las horas de trabajo necesarias para completar una operación.
- La aplicación de políticas coherentes en toda la infraestructura de seguridad (incluyendo, pero sin limitarse a los firewalls).
- Detección de amenazas y gestión del ciclo de vida de la respuesta a incidentes
- Escala (dispositivos gestionados, número de administradores y número de funciones/equipos implicados en las operaciones)
- Gestión de cambios, flujo de trabajo y segregación de funciones

- Automatización y orquestación: Con soluciones de TI y seguridad de terceros, y con la virtualización del centro de datos virtualización, nube y automatización de DevOps;
- Validación y presentación de informes de cumplimiento y control de auditoría.
- Una única construcción de políticas a través de la red, la nube, los endpoints, los móviles y el IoT en la arquitectura.
- Prevención de amenazas y control de acceso unificados en una sola política a través de las instalaciones y la nube
- Validación de control de cumplimiento, con soporte de plantillas para las regulaciones de cumplimiento comunes
- Gestión de amenazas consolidada y procesable e integraciones con los principales proveedores de SIEM y sistemas de gestión de datos Elasticsearch.
- Delegación de autoridad de administración basada en grupos, con soporte completo de flujos de trabajo
- Orquestación de integraciones con entornos virtuales y en la nube, incluida la inserción de servicios automatizados
- API abiertas para potenciar las integraciones de terceros y las herramientas de desarrollo de software y Terraform

3.2. PREVENCIÓN DE AMENAZAS

- Los firewalls deben ofrecer todas las posibles técnicas de prevención de amenazas: sandboxing, antiphishing, antivirus y anti-bot.
- Deben utilizar análisis basados en la nube e inteligencia sobre amenazas en combinación con los firewalls, así como enviar las actualizaciones de prevención de amenazas a los firewalls, y recibir actualizaciones de indicadores de malware para que puedan ser compartidas con otros.
- Debe integrarse con sistemas analíticos y de NAC de terceros (Cisco ISE) que empujan dinámicamente los IoC al firewall, creando un ecosistema más seguro y resistente.
- Deben ofrecer una plataforma basada en la nube que comparte y ofrece inteligencia de seguridad dinámica en tiempo real a la arquitectura de seguridad, incluyendo los firewalls, gateways de seguridad, móviles y endpoints.
- Debe ofrecer motores de IA que detectan el malware mucho más allá de los análisis estáticos y AV, al tiempo que reducen los falsos positivos.
- Sandboxing que bloquea los ataques de día cero antes de que puedan comenzar sus técnicas de evasión.
- Extracción de amenazas (desarme y reconstrucción de contenido) que entrega archivos seguros y limpios a los usuarios protegiéndolos de infecciones. Incluye la extracción de amenazas web y el saneamiento de documentos para las descargas web.
- Anti-phishing que detecta los ataques de phishing y los bloquea antes de que los usuarios puedan infectarse.
- Anti-Ransomware, que detecta y bloquea los ataques de ransomware y restaura los archivos inicialmente cifrados. Prevención de amenazas respaldada por la IA

3.3. INSPECCIÓN Y CONTROL

- El firewall debe tener un soporte de aplicaciones amplio (tantas aplicaciones como sea posible), profundo (subfunciones dentro de las aplicaciones), inteligente (capaz de encontrar la aplicación incluso si se utiliza tecnología de evasión) y dinámico (actualizaciones frecuentes a medida que las aplicaciones proliferan o cambian).
- La capacidad de control de aplicaciones admite políticas de seguridad para identificar, permitir, bloquear o limitar el uso de miles de aplicaciones, incluidas las de la Web y las redes sociales, independientemente del puerto, el protocolo o la técnica de evasión utilizada para atravesar la red.
- Los firewalls deben identificar más de 8,500 aplicaciones Web 2.0, a las cuales se deben añadir otras continuamente.
- Debe proporcionar funciones avanzadas de interacción con el usuario que permitan a los administradores de seguridad alertar a los empleados en tiempo real sobre las limitaciones de acceso a las aplicaciones, y consultarles si el uso de las aplicaciones es para uso empresarial o personal, para conocer mejor los patrones de uso de la Web, adaptar las políticas y regular el uso personal sin interrumpir el flujo del negocio.

3.4. INSPECCIÓN Y CONTROL BASADOS EN LA IDENTIDAD

- Los firewalls deben admitir políticas basadas en usuarios o en grupos de usuarios, que aprovechan el almacén de identidades primario de la organización, normalmente la pertenencia a un grupo de Active Directory.
- La solución debe proporcionar su propio servidor de identidades.
- Debe ofrecer la capacidad de integrarse con Microsoft AD, LDAP, RADIUS, Terminal Servers y con terceros a través de una API web.

3.5. SOPORTE EN LA NUBE

- Los firewalls empresariales deben ofrecer la capacidad para proteger las cargas de trabajo estratégicas, ofreciendo opciones basadas en hardware y software para soportar los entornos de nube híbrida.
- El proveedor también debe abarcar los modelos de gestión de automatización y orquestación en uso, el rendimiento escalable basado en cargas de trabajo dinámicas, y modelos de consumo que permitan un despliegue rentable.
- Los firewalls deben ser compatibles con las implantaciones virtuales y en la nube, además de una completa cartera de dispositivos que abarcan desde los requisitos de las oficinas remotas hasta los centros de datos. La compatibilidad con sistemas virtuales debe permitir segmentar un único Gateway de seguridad de software en varias zonas con recursos y gestión independientes.

- Además de la tradicional vSphere, debe admitir los entornos de red definidos por software NSX. Debe soportar todos los principales proveedores para la nube pública IaaS, como AWS, Azure, GCP, Oracle y Alibaba Clouds. La integración con la automatización de la nube debe proporcionar la instanciación tanto de gateways virtuales como de políticas de seguridad basadas en plantillas sin intervención manual. Esto permite asegurar las nuevas cargas de trabajo a medida que se despliegan, sin retrasos en la implementación causados por la configuración manual de la seguridad.

3.6. RENDIMIENTO ESCALABLE CON FUNCIONES DE SEGURIDAD AVANZADAS

- Los firewalls deben poder escalar fácilmente el rendimiento a medida que aumentan los requisitos, y que las limitaciones de hardware no le impidan desplegar las últimas tecnologías y algoritmos de prevención de amenazas, o que den lugar a consideraciones de rendimiento muy diferentes en despliegues virtuales o en la nube frente a los de hardware.

3.7. INSPECCIÓN DEL TRÁFICO CIFRADO

- Los firewalls deben ser capaces de inspeccionar tráfico cifrado tanto para aplicar la política de control como para la prevención de amenazas. También deben ser lo suficientemente sofisticado como para soportar políticas complejas como el descifrado selectivo para que cierto tráfico pueda excluirse del descifrado para evitar escollos normativos o de responsabilidad.
- El software de firewall empresarial debe permitir el descifrado y la inspección de SSL/TLS, de modo que las políticas de seguridad pueden aplicarse al tráfico cifrado. El software aprovecha la aceleración de hardware integrada en los procesadores. Los firewalls deben categorizar de forma segura el tráfico HTTPS utilizando la extensión Server Name Indication (SNI), inspeccionar todas las suites de cifrado más recientes y curvas como TLS 1.3.

3.8. PREVENCIÓN AUTÓNOMA DE AMENAZAS

- Todos los gateways deben actualizar automáticamente las capacidades de prevención de amenazas basadas en la inteligencia artificial para ofrecer una protección completa incluso contra las amenazas de día cero.
- La política debe permitir a los administradores de seguridad implementar la prevención de amenazas con un solo clic, ofreciendo perfiles out-of-the-box que se ajusten a la red de la SB, la cual se actualiza continuamente de forma automática.

3.9. AUTOMATIZACIÓN DE LA SEGURIDAD

- Los firewalls deben permitir la conexión con el Directorio Activo de Windows o con los sistemas IAM (Identity and Access Management) para crear una política de seguridad basada en el usuario.
- Los firewalls deben poder aprovisionar, configurar e incluir en una orquestación y respuesta de seguridad automatizada (SOAR) ante las amenazas.
- Los firewalls deben proporcionar API abiertas y la adopción de los estándares de la industria, así el autoaprovisionamiento y el autoescalado, junto con las actualizaciones automáticas de políticas, para garantizar que las protecciones de seguridad sigan el ritmo de todos los cambios en los diferentes entornos.
- Los firewalls deben permitir la gestión de la configuración mediante herramientas de terceros como Ansible. Con las herramientas de desarrollo de software, las tareas repetitivas pueden codificarse en flujos de trabajo y conductos CI/CD.

3.10. MONITORIZACIÓN CONSOLIDADA DEL TRÁFICO Y CAPACIDADES DE INDEXACIÓN MEJORADAS

- Los firewalls deben proporcionar unas vistas interactivas ricas y personalizables de todas las actividades de red y de seguridad registradas en los gateways físicos/internos, los gateways basados en la nube, los dispositivos de punto final/móviles y el IoT.
- Deben permitir a los administradores utilizar el panel de vista de logs en bruto, o elegir explorar vistas predefinidas.
- Deben permitir crear paneles personalizables, que proporcionan al administrador una relación de la red y de los eventos basados en diferentes temas como Usuarios remotos, MITRE ATT&CK (utilizando una representación gráfica de un mapa de calor actualizado de MITRE para localizar las técnicas más importantes y desglosar las más relevantes) o Prevención de amenazas.

3.11. INTEGRACIÓN CON NSX

- Integración completa con vCenter y NSX y ofrecer visibilidad total de todos los objetos del centro de datos en la política de seguridad.
- Ofrecer Prevención de Amenazas de Próxima Generación para proteger contra las ciberamenazas y compartir el estado de seguridad de las máquinas virtuales infectadas con NSX para remediación automática.
- Contexto detallado de vCenter y NSX (nombres de VM) en los logs y los eventos.
- Aplicar protecciones de seguridad dentro del centro de datos definido por software:
    - Prevención avanzada de amenazas que protege el tráfico intra-VM
    - Detecta y etiqueta las máquinas virtuales (VM) infectadas, actualiza NSX para la cuarentena y remediación automáticas.
    - La capacidad de seguridad se escala elásticamente para ajustarse a cargas de trabajo de tráfico dinámicas

- Aprovisionamiento de seguridad automatizado y orquestación de seguridad
    - Políticas de seguridad granulares vinculadas dinámicamente a los grupos de seguridad de NSX y a los objetos VM de vCenter para garantizar la seguridad de las aplicaciones virtuales independientemente de los cambios en la topología de la red.
    - Segmentación de las políticas que permita la definición de reglas granulares, automatización y segregación de funciones alineadas con la microsegmentación de NSX.
    - La seguridad se autoaprovisiona a medida que se despliegan nuevos hosts ESX y las máquinas virtuales se mueven dentro del SDDC.
- Visibilidad integral de las amenazas en todo el SDDC
    - Una sola política para los gateways virtuales y físicos, simplificando la aplicación de seguridad.
    - Ofrecer el monitoreo, el registro y el análisis de eventos centralizados que garanticen una visibilidad completa de las amenazas en todo el SDDC.
- La protección de seguridad que proporciona:
    - Prevención de amenazas avanzada de varias capas e inteligencia en tiempo real.
    - La capacidad de seguridad de escalamiento de forma elástica para satisfacer las cambiantes cargas de trabajo de tráfico.
- Análisis forense de las amenazas del tráfico virtual
    - Conservar la identidad de los objetos del centro de datos virtual en logs para facilitar la supervisión y el análisis del tráfico
    - Ofrecer el análisis exhaustivo de eventos de seguridad para detectar anomalías del tráfico virtual y amenazas de día cero
- Aprovisionamiento de seguridad ágil y automatizado
    - Debe estar integrado con NSX y vCenter para extraer dinámicamente los objetos definidos por NSX para políticas de seguridad granulares.
    - Permitir la segmentación de la política de seguridad en subpolíticas para la aplicación a nivel de segmento de red y segregación de funciones
- Gestión unificada de los entornos virtuales y físicos
    - Una única política para los gateways virtuales y físicos simplifica la aplicación de la seguridad
    - Garantizar una visibilidad completa de la postura de seguridad, minimiza la sobrecarga operativa.

4. PRINCIPALES ENTREGABLES

A modo macro se detallan los principales entregables esperados:

- Propuesta de plataforma de Core Firewalls
- Plan de trabajo de implementación de plataforma de Core Firewalls
- Plataforma de Core Firewalls de la Superintendencia de Bancos en funcionamiento

5. PERFIL PROFESIONAL:

- El proveedor o mayorista de la plataforma del Firewall debe tener al menos 05 años de experiencia en el mercado de seguridad implementando Core Firewalls en empresas del sector financiero y proporcionar referencias sobre proyectos exitosos en clientes.

- Los técnicos que participarán en la implementación deben poseer certificados por el fabricante de la solución que valide su capacidad para instalar e implementar este tipo de producto.

- El proveedor debe proporcionar evidencia de liderazgo año tras año en firewalls para empresa, basada en datos independientes de la seguridad de la industria.

Eduard Encarnación
Especialista Senior
Departamento de Seguridad de la Información

Daniel Enrique Leyra
Analista
Departamento de Seguridad de la Información