CONTROL Y PROTECCIÓN TRAFICO DE RED CENTRO DE DATOS

Servicios de Implementación Vmware NSX

Resumen

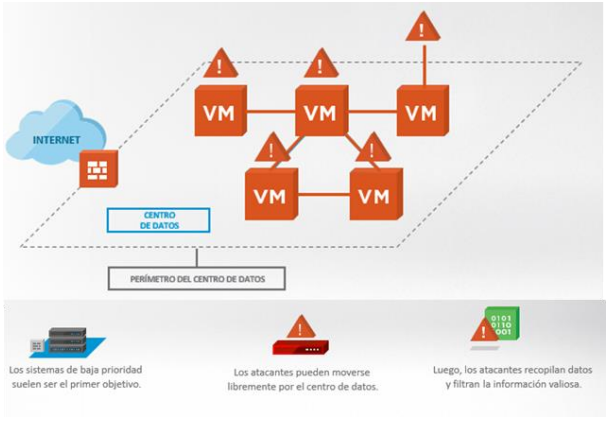
El presente documento describe los objetivos del Proyecto, beneficios, alcances y descripción de los servicios de implementación a través de servicios profesionales de Grupo Sega

La virtualización brinda nuevas oportunidades y nuevos enfoques para optimizar la administración y seguridad de los centros de datos, en esta propuesta nos enfocamos en las tecnologías de seguridad para el ambiente virtual orientadas a la reducción de riesgos informáticos, utilizando Microsegmentación.

La Microsegmentación permite control granular de las comunicaciones en el centro de datos, a nivel de máquina virtual; no es necesario realizar ningún cambio en las aplicaciones que se encuentran en los servidores virtuales, permite control sobre el tráfico de red ***dentro*** del centro de datos, impactando positivamente la continuidad del negocio en los siguientes aspectos:

1. Reducción de riesgos, ataques y amenazas en la comunicación de las aplicaciones, mejorando la continuidad de las mismas.
2. Reducción de costos operativos al automatizar la protección, a través de políticas de seguridad que hacen posible la protección reduciendo complejidad para disponer de tiempo y esfuerzo a otras tareas de seguridad como monitoreo y optimización de las aplicaciones.
3. Reducción de capital, reduciendo la inversión en hardware y equipos de protección perimetral para el ambiente virtual.
4. Aprovisionamiento de protección red inmediata, para la máquina virtual. Esto es un beneficio para el negocio pues se traduce en agilidad para el negocio, tiempo de salida al mercado, entre otros. Importante mencionar que la máquina virtual se puede asegurar de forma automática desde el momento mismo de su creación, al conectarse a la red.

Tradicionalmente en un centro de datos y la red, se manejan segmentos para control del tráfico norte/sur. A través de nuestra propuesta de Microsegmentación para el centro de datos virtual es posible proteger el tráfico este/oeste**,** que se genera dentro del centro de datos virtual.



Microsegmentación

Con la microsegmentación se presenta el concepto donde cada máquina virtual tiene su propio firewall el cuál tiene las siguientes características:

- Implementación basada en kernel para entregar alto desempeño
- Existe por fuera de la máquina virtual garantizando la seguridad apropiada
- Todos los firewalls tienen un único punto de gestión evitando la administración individual
- El firewall posee todo el contexto del entorno virtual, por lo que las políticas se mantienen actualizadas a pesar de los cambios en el entorno

Nuestra oferta de servicio puede abarcar desde la preparación del centro de datos para el cumplimiento de los requerimientos minimos; hasta una implementación completa de todas las características que permitan mantener un centro de datos protegido, de forma adecuada a las nuevas amenazas. Algunos de los servicios que podemos cotizar son:

- Implementacion de Switches distribuidos
- Despliegue de NSX con caso de uso Microsegmentación
- Migración de hipervisores
- Creación de agrupaciones dinámicas en service composer
- Creación de políticas de seguridad basadas en service composer
- Generación de procedimiento para identificación de flujos de comunicación
- Configuración de reporte a herramientas de syslog incluyendo loginsight que viene incluido en la versión 6.2.3 de NSX.
- Desplegar Guest Introspection Appliances para funcionalidad de Activity Monitoring
- Activación del servicio de flow monitoring

Beneficios de la solución

- Reducción de costos operativos y de gestión.
- Reducción de tiempos de aprovisionamiento de una red para una nueva aplicación, de 3-4 semanas a minutos
- Maximizar el potencial de la infraestructura de la data center, permitiendo optimizar hasta un 85% su nivel de uso
- Ganar tiempo en Time to Market de la aplicación a publicar por medio de la automatización.
- Aplicar alta disponibilidad y tolerancia a fallos a las aplicacione publicadas por medio de balanceo de carga dentro de la granja de ervidores Front-End.
- Ahorro hasta en un 68% en Capex, gracias al control y optimización del tráfico realizados dentro del ambiente virtual, permitiendo extender la vida y el uso de los switches y firewalls del data center

VNA – Assessment Gratuito

Grupo Sega ofrece un análisis de los flujos actuales de comunicación en su centro de datos, este análisis denominado VNA (virtual Network Assessment) y requiere:

- vCenter y ESXi 5.5, actualización 2 (versión 2068190) y posteriores, o
- vCenter y ESXi 6.0, actualización 1b (versión 3380124) y posteriores, o
- vCenter y ESXI 6.5a o superiores
    - El switch virtual distribuido (vDS) es **OBLIGATORIO**.
    - Durante la configuración, la cuenta debe modificar los permisos para configurar IPFIX:
        - ***Switch distribuido:*** **modificar**
        - ***Grupo de puertos virtuales distribuidos:*** **modificar**
    - SSH, HTTPS y SNMP (v2c &y v3) para todos los enrutadores, switches y firewalls de hardware que estén conectados a la plataforma de vSphere.
        - ***Nota***: Se puede realizar la evaluación sin acceder a dispositivos físicos. Sin embargo, el informe quedará incompleto.
    - Fuente de entrada opcional (si existe, mejor, pero **NO** es obligatoria): NSX 6.2 o superior (el soporte de la versión 6.1.x finalizó en enero de 2017)
    - Consulte las Matrices de interoperabilidad de productos de VMware.

Se desplegarán dos appliances virtuales, los cuyos requerimientos son:

- Plataforma de vRealize Network Insight
    - 8 núcleos (reserva en 4096 Mhz)
    - 32 GB de memoria RAM (reserva de 16 GB)
    - 750 GB de HDD (aprovisionamiento ligero)

Proxy de vRealize Network Insight

- 4 núcleos (reserva en 2048 Mhz)
- 10 GB de memoria RAM (reserva de 5 GB)
- 150 GB de HDD (aprovisionamiento ligero)