SONICWALL

RESUMEN EJECUTIVO: 4 OBSTÁCULOS QUE DIFICULTAN LA SEGURIDAD DE LA NUBE PÚBLICA/PRIVADA

Examinamos las trampas de seguridad que amenazan a los entornos virtuales de hoy en día

Resumen

Si bien la virtualización y la nube pueden reducir costes y aumentar la eficiencia y la agilidad operacional, también se enfrentan a amenazas de malware cada vez mayores. El departamento de TI cuenta con presupuestos limitados para proteger los entornos de nube pública/privada contra las trampas de seguridad más comunes, como son las siguientes:

- Falta de visibilidad del tráfico entre equipos virtuales
- Proliferación de políticas
- Expansión virtual excesiva
- Limitaciones de la nube pública

La virtualización como factor de éxito

Las organizaciones, que hacen frente a mercados de rápida evolución, a una dura competencia y a un entorno de negocio acelerado, deben proteger su cuota de mercado y crecer al mismo tiempo. Hoy más que nunca, la tecnología de la información desempeña un papel principal.

En el back end, se espera que los responsables de TI sigan el ritmo de las innovaciones tecnológicas, modernicen los centros de datos y el entorno de TI y optimicen los servicios de TI para hacer posible el éxito de la organización. Esto incluye el diseño, la implementación y el despliegue de nuevas aplicaciones de negocio, herramientas y servicios que favorezcan la productividad de los usuarios y arquitecturas de red como la computación en nube privada/pública/híbrida, la virtualización de las funciones de red y la movilidad. Al mismo tiempo, el equipo de TI debe soportar y proteger este entorno de red dinámico y al personal móvil con un presupuesto fijo, que puede ser muy reducido.

En el front end, el departamento de TI debe asegurarse de que las interacciones, los servicios y el soporte Web de la empresa estén online las 24 horas del día los 365 días del año. Esto implica mantener todos los recursos Web de la organización a salvo, sin interrupciones y rindiendo al máximo. Los responsables de TI buscan una defensa de seguridad asequible pero sin compromisos. Ello requiere seguridad dinámica capaz de prevenir ataques al tiempo que proporciona los análisis necesarios para proteger y responder en toda la infraestructura física y virtual de la organización. El personal de TI debe insistir en lograr una seguridad sin compromisos, ya sea a través de una nube por cable/inalámbrica o privada/pública y desde las oficinas centrales hasta los campus remotos, sucursales, filiales o entornos de partners.

Ventajas e inconvenientes de la virtualización

Desde hace más de una década, la virtualización de los servidores está favoreciendo una infraestructura de TI cada vez más inmaterial. Actualmente, la virtualización sigue desempeñando un papel importante, ya que continúa avanzando y aumentando las ventajas operacionales y económicas de todo el centro de datos, reduciendo tanto los gastos operativos como los de capital y permitiendo al personal centrarse en la infraestructura crítica.

Los continuos avances en las herramientas y los servicios de virtualización, como la virtualización de las funciones de red, están permitiendo a los departamentos de TI desarrollar y colocar cargas de trabajo virtualizadas en cualquier lugar de la red virtual de forma rápida y sencilla. Además, la virtualización proporciona a los responsables de TI más prestaciones de programabilidad de red y autogestión, así como la velocidad de aprovisionamiento que necesitan para ejecutar el centro de datos con mayor eficiencia. De este modo, los equipos de redes y aplicaciones pueden crear nuevos servicios a medida, entregarlos e inmediatamente iniciar, mover, copiar, clonar, restaurar o eliminar esos servicios hospedados en equipos virtuales en cualquier momento para satisfacer las necesidades específicas de sus centros de datos. Este mayor nivel de agilidad y elasticidad operacionales reduce considerablemente el coste de la entrega de servicios de aplicaciones a toda la empresa.

Sin embargo, a pesar de todas estas ventajas, el inconveniente de utilizar tecnología de virtualización radica en las numerosas implicaciones y preocupaciones de seguridad a las que debe hacer frente el equipo de TI. (Ver tabla 2 abajo). La virtualización, por su naturaleza, añade múltiples capas de complejidad a nivel de infraestructura y operacional. Cuestiones como el uso compartido del almacenamiento, el enrutamiento de dispositivos, los segmentos de red y los canales de comunicación han demostrado ser vulnerables a los ataques cibernéticos como los ataques de uso indebido de recursos compartidos, ataques entre equipos virtuales, ataques de canal lateral y vulnerabilidades comunes de aplicaciones y protocolos basadas en la red. Estas amenazas llegan a todas las partes del framework virtual, incluidos el hipervisor o el monitor del equipo virtual, los equipos virtuales, los sistemas operativos de los equipos virtuales, las aplicaciones ejecutadas en esos sistemas operativos y los componentes de redes virtuales o del entorno virtualizado. Proteger todo el entorno virtual de forma inapropiada podría causar daños incalculables a la organización.

Tabla 2 Relaciones entre las vulnerabilidades y las amenazas en entornos de virtualización de redes

Categorías de amenazas		Vulnerabilidades	Amenazas
Revelación de información	Filtración de información	Falta de protección de tablas ARP	Envenenamiento de tablas ARP
		Implementación de normas de firewall dentro de nodos virtuales	Subversión de normas de firewall
	Intercepción de información	Falta de protección de tablas ARP	Envenenamiento de tablas ARP
		Transmisión de datos en patrones predecibles	Ataques de análisis de tráfico
		Manejo de múltiples solicitudes secuenciales no controladas de redes virtuales desde una única entidad	Inferencia y revelación de información topológica sensible
		Intercambio no protegido de información de enrutamiento entre routers virtuales	Revelación de información de enrutamiento sensible
	Explotación de la información introspectiva	Introspección no controlada	Robo de datos
Engaño	Fraude de identidad	Manejo inapropiado de identidades:	
		- dentro de redes individuales	Inyección de mensajes maliciosos con fuentes falsificadas
		- entre redes federadas	Escalación de privilegios
		- durante procedimientos de migración	Abuso de eliminación de nodos y reagregación de los mismos a fin de obtener nuevas identidades (limpias)
	Pérdida de entradas de registro	Operaciones de reversión no controladas	Pérdida de entradas de registro
	Ataques de reproducción	Falta de identificadores de mensajes únicos	Ataques de reproducción
Interrupción	Sobrecarga de recursos físicos	Asignación de recursos no controlada	Degradación del rendimiento
			Consumo abusivo de recursos
		Manejo no controlado de solicitudes de redes virtuales	Agotamiento de recursos en partes específicas de la infraestructura
		Falta de estrategias de recuperación proactiva o reactiva	Ataques por denegación de servicio
	Fallo de recursos físicos	Falta de estrategias de recuperación proactiva o reactiva	Fallo de routers/redes virtuales
		Asignación de recursos no controlada tras fallos	Sobrecarga de routers virtuales restantes tras fallos
Usurpación	Fraude de identidad	Manejo inapropiado de identidades y privilegios asociados	Escalación de privilegios
	Explotación de vulnerabilidades de software	Escalación de privilegios en monitores de equipos virtuales	Control no autorizado de routers físicos

Fuente: "Virtual network security: threats, countermeasures, and challenges," Journal of Internet Services and Applications, Dic. 2015

Estos daños pueden incluir:

- Uso no autorizado de los sistemas virtuales para ejecutar acciones maliciosas
- Acceso no autorizado a los recursos de datos protegidos
- Robo de información
- Interrupción del servicio o degradación de parte del ecosistema virtual

Actualmente, la virtualización es un campo activo de investigación de vulnerabilidades y amenazas en los ámbitos académico, de las recompensas por la detección de errores, el hackeo ético y el crimen cibernético organizado. Se descubren nuevas amenazas regularmente. VENOM, CVE-2015-3456, es un ejemplo de un exploit que afecta a plataformas de virtualización populares, como Xen y KVM.

Los responsables de TI, por tanto, tienen motivos para estar profundamente preocupados por la seguridad. A muchas organizaciones les preocupa que sus sistemas de defensa actuales carezcan de las prestaciones y los controles de seguridad dinámicos necesarios para proporcionar una protección continua apropiada para las infraestructuras de las redes virtuales. Como consecuencia, garantizar la continuidad de las operaciones, la entrega y la disponibilidad de los servicios y el cumplimiento normativo constituye todo un reto para los responsables de TI.

Escenario práctico

Con el fin de ofrecer una perspectiva más práctica, examinemos un escenario en el que el entorno virtual de una organización se encuentra instalado en una arquitectura de seguridad de firewall físico. La Figura 1 (arriba derecha) describe el canal del flujo de comunicación desde el equipo virtual de la aplicación hasta el equipo virtual de la base de datos en el equipo virtual huésped. La aplicación podría ser un SharePoint de Microsoft realizando una lectura/escritura a una base de datos SQL. En este caso, los responsables de TI deben asegurarse de que los servicios de la aplicación se entreguen de forma segura.

Entorno virtual con firewall físico

Los responsables de TI cuentan con dos posibles enfoques de inspección con métodos antiguos existentes. Una opción consiste en enrutar el tráfico entre equipos

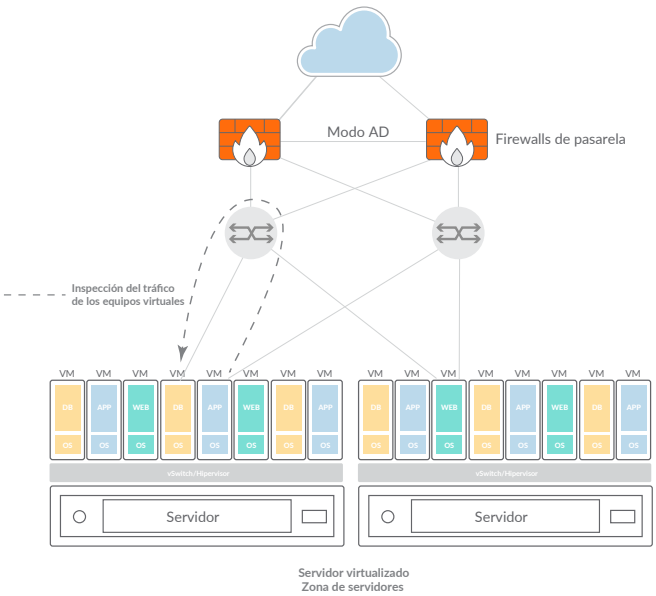

Figura 1: Entorno virtual con firewall físico

virtuales mediante el switch virtual (vSwitch) dirección norte a la estructura de conmutación externa, y después a un firewall externo que a continuación devuelve los datos por el mismo canal en dirección sur. Direccionar el tráfico de esta manera requiere numerosos hops, y puede causar problemas como la degradación del rendimiento, latencia, pérdida de paquetes y preocupaciones relacionadas con el control de la seguridad, tal y como se define más arriba. El segundo enfoque consiste en utilizar firewalls basados en software y ejecutarlos como agentes en cada equipo virtual. Este método se enfrenta a retos similares, con un rendimiento pobre, y una complejidad de gestión que aumenta a medida que crece el volumen de los equipos virtuales.

A la hora de examinar los retos de seguridad de los firewalls físicos en un mundo virtualizado dinámico, las trampas comunes a las que se enfrentará el departamento de TI son las siguientes:

1. Falta de visibilidad del tráfico entre equipos virtuales
2. Proliferación de políticas
3. Expansión virtual excesiva
4. Entorno de nube pública

Falta de visibilidad del tráfico entre equipos virtuales

Si tiene decenas de equipos virtuales en un sistema virtual con comunicación entre ellos, es posible que un firewall perimetral físico no vea el tráfico lateral, puesto que el tráfico posiblemente nunca salga del servidor virtual debido a los aislamientos o a las configuraciones de enrutamiento del equipo virtual. Desde el punto de vista de la seguridad, esto significa que la monitorización para detectar eventos inusuales y anomalías en estos escenarios se vuelve imposible.

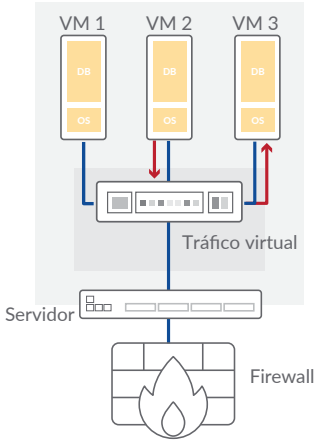

Figura 2: Tráfico entre equipos virtuales

Proliferación de políticas

La creación o el traslado de recursos virtualizados requiere numerosos cambios complejos en la configuración de las redes con el fin de dirigir el tráfico de esos equipos virtuales al firewall físico. Esto implica reglas de enrutamiento y de NAT, puertos y protocolos soportados por la aplicación. Las directrices de gestión de cambios exigen que los cambios de políticas se sometan a un proceso manual y laborioso de flujo de trabajo de examen, aprobación, auditoría y prueba antes del lanzamiento de producción. Esto no solo resulta altamente ineficiente y caro, sino que además afecta negativamente a las operaciones debido a la gran cantidad de gente implicada.

Además, con las nuevas reglas que se suman a los cientos de reglas oscuras que tal vez nunca hayan sido auditadas ni autorizadas, las políticas de seguridad se vuelven muy complicadas e ingestionables. Los responsables de TI podrían empezar a ver cómo aparecen, o crecen, brechas en las políticas, amenazas que pasan desapercibidas y/o una caída del rendimiento.

Expansión virtual excesiva

La expansión virtual excesiva hace referencia al frecuente problema que se produce cuando el elevado número de recursos virtuales de un entorno hace que sea demasiado complejo hacer un seguimiento del mismo y controlarlo. Cuando se copian, clonan o trasladan equipos virtuales (y en muchos casos, se suspenden y se olvidan), surgen riesgos de seguridad, y el entorno queda abierto y vulnerable, puesto que las políticas y los controles ya no funcionan adecuadamente. Por este motivo, no resulta práctico tener una regla de seguridad fija para una dirección IP estática de un equipo virtual, dado que las direcciones IP de los equipos virtuales a menudo cambian. Se trata de un problema extendido, y los hackers están explotando activamente las vulnerabilidades. Por tanto, un entorno virtual dinámico requiere controles de seguridad dinámicos, con un proceso de cambios estrechamente regulado y auditable para asegurar que los equipos virtuales se adhieran a las políticas de seguridad y configuración apropiadas.

Entorno de nube pública

Otro caso de uso problemático se produce cuando los servicios de las aplicaciones de una organización se encuentran en la nube pública, como Amazon Web Services (AWS) o Microsoft Azure. En un entorno de nube, los responsables de TI de la organización no pueden poner un dispositivo de firewall físico en el centro de datos protegido del proveedor. Se trata de instalaciones extremadamente controladas. Incluso si el equipo de TI pudiera colocar un dispositivo físico en ellas, simplemente no podría dictar el patrón del tráfico, de modo que el firewall estaría delante del tráfico de aplicaciones de la organización. En este caso, el firewall también debe ser virtual, de manera que los responsables de TI puedan utilizar redes definidas por software o configuraciones manuales para permitir a los ingenieros de tráfico colocar el firewall virtualizado entre sus servicios de aplicaciones y el resto del mundo, tanto si la ruta es interna como externa al centro de datos.

Conclusión

Al analizar la relación coste-beneficio de una iniciativa de virtualización, la seguridad debería ser siempre un factor clave. Las ventajas, como el ahorro y la mayor eficiencia, deben ponderarse frente a los posibles daños causados por las amenazas crecientes y los peligros frecuentes. El equipo de TI debe explorar nuevas soluciones que vayan más allá de las tecnologías y los enfoques antiguos y que pueden garantizar de forma efectiva el éxito de la seguridad de la virtualización.

Más información: Lea nuestro resumen de la solución "Qué debe ofrecer un firewall virtual de próxima generación" y visite www.sonicwall.com/virtual-firewall.

Acerca de nosotros

SonicWall lleva más de 25 años combatiendo la industria del crimen cibernético, defendiendo a las empresas pequeñas, medianas y grandes de todo el mundo. Nuestra combinación de productos y partners nos ha permitido crear una solución de defensa cibernética en tiempo real adaptada a las necesidades específicas de más de 500.000 negocios en más de 150 países, para que usted pueda centrarse por completo en su negocio sin tener que preocuparse por las amenazas.

Si tiene alguna duda sobre el posible uso de este material, póngase en contacto con nosotros:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Para más información, consulte nuestra página Web.
www.sonicwall.com