



Virtualización de la seguridad en el gateway del correo electrónico

Protección flexible y rentable en el gateway del correo electrónico

Agosto de 2009





VIRTUALIZACIÓN DE LA SEGURIDAD EN EL GATEWAY DEL CORREO ELECTRÓNICO

I. EL COSTE Y LA COMPLEJIDAD MUEVEN LOS INTENTOS DE VIRTUALIZACIÓN

Las iniciativas de virtualización han adquirido protagonismo al tiempo que las empresas buscan formas de reducir los costes y la complejidad de las operaciones, enfrentadas a una situación económica débil y al aumento de los costes de energía. En muchas organizaciones se están tomando iniciativas de TI respetuosas con el medio ambiente para ayudar a reducir los efectos del aumento de los costes en el balance general de la empresa. Al mismo tiempo, unas infraestructuras de TI cada vez más complejas exigen más tiempo y recursos para su gestión, factores que ya escasean. La virtualización constituye un método para ayudar a las organizaciones a hacer frente a estas exigencias.

AUMENTO DE LOS COSTES DE LA ENERGÍA

Hoy en día, los centros de datos consumen casi un 1% del suministro de electricidad del planeta, y se espera que el consumo se cuadruplique antes de 2020. La electricidad representa en la actualidad al menos el 25% de los costes de TI de una organización (*Revolutionizing Datacenter Efficiency*, McKinsey & Company Uptime Institute Symposium) y, con la necesidad de mantener niveles de servicio siempre al día para aplicaciones empresariales básicas, es muy probable que ese porcentaje aumente. Incluso aunque los centros de datos mantengan los niveles actuales de uso de electricidad, los costes irán creciendo conforme se dispare la demanda mundial y aumenten los precios de los combustibles, tales como carbón y gas natural, en respuesta a esa demanda.

DESGASTE DEL HARDWARE

Conforme ha ido aumentando la complejidad de las infraestructuras a lo largo de los últimos años, muchas organizaciones de TI han hecho frente a cada reto con una nueva solución. Se han saturado con una gran cantidad de pequeños appliances de hardware dedicados a resolver sencillos problemas. La implementación y gestión de nuevos servidores o de appliances de hardware dedicados para cada una de estas aplicaciones contribuye a aumentar aún más los costes y la complejidad que implica mantener el centro de datos. Además de la creciente necesidad de espacio de bastidor, las organizaciones de TI se encuentran con una miríada de servidores y appliances de hardware con distintas interfaces difíciles de gestionar.

ENTORNOS DE SERVIDOR COMPLEJOS

En las implementaciones de servidor tradicionales, se necesita por lo general de un largo ciclo de adquisición, instalación, configuración, prueba e implementación, lo que ralentiza la capacidad de una organización para implementar aplicaciones básicas. Al mismo tiempo, son pocos los servidores que se utilizan al completo, lo que aumenta el coste total de la propiedad. Los equipos virtuales son más eficaces y sencillos de implementar que los servidores físicos y el software tradicional.



VIRTUALIZACIÓN DE LA SEGURIDAD EN EL GATEWAY DEL CORREO ELECTRÓNICO

II. AMPLIACIÓN DE LA VIRTUALIZACIÓN A MÁS FUNCIONES DE LOS CENTROS DE DATOS

Con unos costes iniciales y de funcionamiento significativamente inferiores, el cambio a la infraestructura de virtualización está ganando peso. La adopción de una infraestructura virtualizada simple puede reducir los costes anuales de servidor por usuario en hasta un 35%, en comparación con una configuración de servidor x86 estática física. Las infraestructuras con más de un 25% de herramientas de virtualización, virtualización de almacenamiento y gestión de sistemas pueden reducir los costes en hasta un 52% por usuario y año (*IDC, Business Value of Virtualization: Realizing the Benefits of Integrated Solutions*, julio de 2008).

Por este motivo, el concepto de virtualización está traspasando las barreras de la simple virtualización de servidores que albergan aplicaciones Web y empresariales, para aplicarse a otras funciones de los centros de datos, tales como las aplicaciones de seguridad del gateway de red.

¿QUÉ SON LOS APPLIANCES VIRTUALES?

Un appliance virtual incluye un sistema operativo previamente instalado y configurado y aplicaciones que se empaquetan, implementan y mantienen, actualizan y gestionan como una sola unidad que funciona en una plataforma virtualizada. Al estar ya empaquetadas, estas aplicaciones simplifican la implementación y la administración, ya que la aplicación de parches y actualizaciones procede de un solo proveedor. Como no se necesita proporcionar electricidad, refrigeración ni hardware extra, los appliances virtuales pueden proporcionar funciones adicionales con un impacto medioambiental añadido mínimo o inexistente. Las organizaciones están implementando appliances virtuales para funciones que abarcan desde la inteligencia empresarial y la gestión de documentos hasta las copias de seguridad, la supervisión de redes, la implementación de aplicaciones y la seguridad.

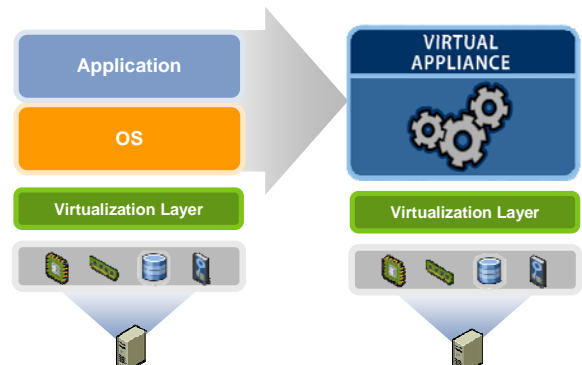


Ilustración 1: Un appliance virtual incluye una aplicación y un sistema operativo en forma de unidad cohesionada

¿POR QUÉ UTILIZAR APPLIANCES VIRTUALES PARA LAS APLICACIONES DE SEGURIDAD DEL CORREO ELECTRÓNICO EN EL GATEWAY?

La seguridad en el correo electrónico es el objetivo idóneo para ahorrar costes y aumentar la eficacia de una implementación de appliances virtuales. El correo electrónico es vital para la actividad empresarial diaria, razón por la cual, incluso en épocas de crisis económica, casi el 60% de las empresas tienen planeado invertir en seguridad para el correo electrónico, según IDC. El spam no cesa de proliferar, lo que sobrecarga rápidamente los servidores físicos y afecta a los recursos de gestión; además, debido a las fluctuaciones extremas que se dan en los volúmenes de



VIRTUALIZACIÓN DE LA SEGURIDAD EN EL GATEWAY DEL CORREO ELECTRÓNICO

spam, las necesidades de capacidad de los servidores resultan impredecibles. Las organizaciones deben enfrentarse a difíciles elecciones entre gastos imprevistos en un aumento de la capacidad para minimizar el impacto de altos volúmenes de spam en el negocio y hacer frente a una disminución del rendimiento y la satisfacción del usuario.

Muchas organizaciones pretenden utilizar appliances virtuales para lograr sus objetivos en cuanto a seguridad en el gateway del correo electrónico. Osterman Research calcula que, antes de 2010, hasta el 39% de los servidores antivirus y antispam serán virtuales (*Why You Need to Consider Virtualization*, septiembre de 2008). Además, IDC concluyó que el 34% de las organizaciones pretenden adoptar appliances de seguridad virtuales para la seguridad en el correo electrónico dentro de los próximos 12 meses, y que las grandes organizaciones (de más de 10 000 empleados) serán quienes más lo hagan: un 48% (estudio sobre seguridad en mensajería de IDC: *The Good, Bad, and Ugly*, febrero de 2009). Los appliances de seguridad virtuales también serán el segmento de crecimiento más rápido en el mercado de la seguridad para mensajería, con un aumento de 17 millones de dólares en 2008 a 525 millones de dólares en 2013, lo que representa un 98% de la tasa compuesta de crecimiento anual (*IDC Worldwide Messaging Security 2008 Vendor Shares and 2009-2013 Forecast*).

VENTAJAS DE IMPLEMENTAR UN APPLIANCE VIRTUAL EN VMWARE

Los appliances virtuales de seguridad para mensajería en un entorno VMware ofrecen las mismas ventajas en cuanto a costes en el gateway que las que ofrecen las soluciones virtualizadas para otras necesidades de los centros de datos; a saber: reducción de costes, menor impacto, gestión simplificada y facilidad de implementación. También proporcionan la ventaja añadida de reducir significativamente los costes iniciales y los de mantenimiento y gestión, lo que redundará en un menor coste total de propiedad en comparación con las soluciones tradicionales de protección del gateway del correo electrónico.

La implementación y gestión simplificadas ahorran tiempo

Con un appliance virtual, el tiempo necesario para configurar, instalar, aplicar parches y probar se ve reducido, lo que disminuye los costes generales de administración y gestión. La aplicación de parches a todo el appliance virtual (tanto a la aplicación como al sistema operativo) tiene lugar de forma automática y desde un solo proveedor, lo que reduce aún más la cantidad de tiempo de gestión necesario. VMware vCenter Server proporciona funciones de supervisión y controles de salud de los appliances virtuales en el entorno VMware, lo que simplifica la gestión.

Continuidad del negocio para la protección del gateway del correo electrónico

Los appliances virtuales de seguridad para la mensajería, basados en las funciones de gran disponibilidad y escalabilidad de VMware, también pueden desempeñar un papel clave a la hora de apoyar las estrategias de continuidad del negocio. VMware Data Recovery, además, permite hacer copias de seguridad y recuperar los datos de forma rápida y sencilla en los equipos virtuales.



VIRTUALIZACIÓN DE LA SEGURIDAD EN EL GATEWAY DEL CORREO ELECTRÓNICO

Protección de gran disponibilidad en el gateway del correo electrónico

Los appliances virtuales de seguridad para mensajería también están diseñados para su implementación en empresas a gran escala. Los entornos VMware Infrastructure y VMware vSphere ofrecen resiliencia para todos los componentes de un appliance virtual, lo que permite a las empresas cumplir con sus objetivos de TI en cuanto a fiabilidad, escalabilidad, redundancia y disponibilidad. Los appliances virtuales de seguridad para mensajería también aprovechan las funciones de VMware para empresas distribuidas, lo que incluye:

- **VMware VMotion:** elimina la necesidad de programar tiempos de inactividad de las aplicaciones debida a operaciones planificadas de mantenimiento de servidores, gracias a la migración en vivo de los equipos y appliances virtuales a través de los servidores, sin que los usuarios se vean afectados por posibles interrupciones ni se pierda el servicio.
- **VMware Fault Tolerance:** ofrece una disponibilidad continua, sin pérdidas de datos ni tiempos de inactividad, a appliances y aplicaciones virtuales.
- **VMware High Availability:** permite reiniciar todas las aplicaciones de forma eficaz y automática, en cuestión de minutos, en caso de fallo del hardware o del sistema operativo.

ESCALABILIDAD PARA ENTORNOS EN CLÚSTER

VMware Infrastructure y VMware vSphere admiten también una escalabilidad infinita de la protección en el gateway del correo electrónico para entornos en clúster. Los administradores de los centros de datos pueden prestar asistencia a más usuarios con menos esfuerzo, al tiempo que ayudan a garantizar un alto rendimiento. VMware Distributed Resource Scheduler supervisa constantemente el uso a través de los grupos de recursos y equilibra de forma dinámica la carga de los recursos de los servidores para ofrecer los recursos apropiados a los appliances virtuales de seguridad para mensajería, lo que maximiza la protección basada en la prioridad empresarial.

III. APPLIANCES Y APLICACIONES VIRTUALES PARA LA INFORMÁTICA EN INTERNET

La iniciativa vCloud de VMware permite disponer de actividades informáticas en Internet de nivel empresarial, al federar la capacidad informática bajo petición entre los centros de datos virtuales y los proveedores de servicios en Internet para dar cabida a aplicaciones existentes y nuevas. Esta iniciativa está destinada a ayudar a las empresas, tanto grandes como pequeñas, a utilizar de forma segura su capacidad informática dentro y fuera de sus cortafuegos (cuando, como y cuanto quieran) para asegurar la calidad del servicio para cualquier aplicación que deseen ejecutar, ya sea de forma interna o como servicio.

Además, la iniciativa vCloud de VMware puede aprovechar el amplio abanico de aplicaciones que admiten los proveedores de software que se ejecutan en VMware, así como el creciente ecosistema de appliances virtuales de VMware Ready. Con los appliances virtuales de VMware



VIRTUALIZACIÓN DE LA SEGURIDAD EN EL GATEWAY DEL CORREO ELECTRÓNICO

Ready, la implementación de aplicaciones nuevas en Internet o in situ se convierte en una tarea muy sencilla. Los socios de VMware, como Trend Micro, están aprovechando los appliances virtuales de VMware Ready para permitir una fácil aplicación de parches, gestión y migración de aplicaciones dentro y fuera de los servicios en Internet.

Para garantizar una transición gradual a las estrategias en Internet, VMware ha presentado sus vApp, la próxima generación de appliances virtuales. Un vApp es una solución de software preinstalada que consta de varios equipos virtuales, empaquetados y mantenidos como una sola entidad en el estándar OVF (Open Virtualization Format, Formato de virtualización abierto) del sector. Los vApps, por lo general, encapsulan todos los componentes de una aplicación compleja de varias capas, así como las políticas de funcionamiento y los niveles de servicio asociados a ésta. Los vApps, que se definen mejor como entidades que se autogestionan y autodescriben, están compuestos de todas las aplicaciones que se ejecuten en cualquier sistema operativo y ofrecen un mecanismo para que los clientes muevan sus aplicaciones entre entornos de Internet internos o externos al tiempo que mantienen los mismos niveles de servicio. Esto los convierte en contenedores ideales para la informática en Internet. Los vApps pueden crearse y gestionarse con VMware vSphere 4.0.

IV. EL APPLIANCE VIRTUAL DE SEGURIDAD PARA MENSAJERÍA DE TREND MICRO, VMWARE READY

Trend Micro y VMware están ayudando a sus clientes a lograr transformar sus centros de datos al maximizar sus iniciativas de virtualización con soluciones seguras y flexibles. El appliance virtual InterScan™ Messaging Security de Trend Micro™, está validado para VMware Ready para complementar entornos virtualizados con una protección exhaustiva del correo electrónico en el gateway. Las soluciones VMware Ready aseguran interoperabilidad en la línea de base y mayores niveles de integración con los productos VMware. Gracias al logotipo de VMware, los clientes saben que el appliance de Trend Micro cumple con los criterios especificados por VMware y está optimizado para el sistema operativo Virtual Datacenter de VMware.

El appliance virtual InterScan Messaging Security de Trend Micro puede implementarse como appliance virtual dedicado en hardware "bare metal" estándar del sector o bien como appliance virtual de VMware Ready para su implementación en entornos VMware ESX/Infrastructure.



VIRTUALIZACIÓN DE LA SEGURIDAD EN EL GATEWAY DEL CORREO ELECTRÓNICO

V. SEGURIDAD VIRTUAL EXHAUSTIVA PARA EL CORREO ELECTRÓNICO EN EL GATEWAY

SPAM MULTICAPA, PROTECCIÓN FRENTE A PHISHING Y CIFRADO OPCIONAL

Trend Micro Smart Protection Network™ utiliza una combinación de servicios de reputación en Internet para bloquear una gran parte del correo electrónico malicioso antes de que éste pueda alcanzar el gateway de las instalaciones de la empresa. Las defensas integradas en el appliance virtual realizan un análisis en profundidad del correo electrónico utilizando varias técnicas de vanguardia, como, por ejemplo, la detección de spam con imágenes (pendiente de patente), la identificación de URL maliciosas incrustadas y otros sistemas de defensa actualizados al minuto, para contener nuevas técnicas de spam. Las organizaciones pueden aplicar servicios de reputación y perfiles automáticos que detienen el spam y los virus y crean un cortafuegos frente a los ataques de DHA y correo electrónico rebotado. El appliance virtual InterScan Messaging Security utiliza, además, servicios de reputación, firmas y modelos heurísticos para detener el phishing, incluidos los ataques de phishing dirigidos a empresas.

ANTIVIRUS Y ANTISPYWARE GALARDONADOS

Trend Micro detiene los virus y el spyware ocultos en los archivos adjuntos de correo electrónico. El appliance virtual InterScan Messaging Security, que cuenta con Smart Protection Network™, ofrece una protección inmediata que funciona como un servicio de vigilancia virtual. La base de datos de reputación Web exclusiva de Trend Micro recopilan información sobre amenazas a través de una red mundial de clientes, desde clientes individuales hasta grandes empresas. Cada ataque producido en un PC determinado se añade a la base de datos (lo que hace más preciso el conocimiento de Trend Micro acerca de la reputación de un sitio Web, el funcionamiento del malware y las fuentes de spam) y permite ofrecer una protección casi inmediata.

FILTRADO DE CONTENIDOS FLEXIBLE

Los mensajes y archivos adjuntos de correo electrónico entrante y saliente se exploran en busca de contenido inapropiado y pérdidas de datos confidenciales, basándose en características de archivos adjuntos, glosarios predefinidos, identificadores y reglas de datos personalizables. El appliance virtual InterScan Messaging Security ofrece opciones de limpieza flexibles, entre las que se encuentran renuncias de responsabilidad legal específicas de las empresas, la cuarentena de mensajes de correo electrónico y la emisión de alertas; permite dirigir políticas a remitentes o destinatarios por empresa, grupo o persona individual y es compatible con la prevención frente a pérdida de datos, el cumplimiento de políticas y las iniciativas de normativas corporativas.



VIRTUALIZACIÓN DE LA SEGURIDAD EN EL GATEWAY DEL CORREO ELECTRÓNICO

VI. LOS CLIENTES SE PASAN AL APPLIANCE VIRTUAL DE TREND MICRO

Los clientes de Trend Micro están ampliando sus estrategias de virtualización para incluir la protección virtual del correo electrónico en el gateway, por medio del appliance virtual InterScan Messaging Security de Trend Micro.

OCHSNER HEALTH SYSTEM

Ochsner Health System es un sistema académico, sin ánimo de lucro, de prestación sanitaria en diversas especialidades, situado en el sureste del estado de Louisiana (EE.UU.). Para gestionar los costes según va creciendo la empresa, el departamento de TI ha emprendido varias iniciativas de ahorro, entre las que se incluye la consolidación de sus servidores de correo electrónico. Su solución de seguridad para el correo electrónico en el gateway, basada en hardware, no se podía escalar de forma eficaz y, cuando el departamento de TI estudió las distintas alternativas, decidió que quería que su nueva solución se integrara bien en su entorno virtualizado VMware. Ochsner eligió el appliance virtual InterScan Messaging Security de Trend Micro, porque contaba con la certificación VMware Ready y ofrecía una gran disponibilidad y funciones de recuperación frente a desastres en la comunicación mediante correo electrónico.

“Era muy importante que Trend Micro InterScan Messaging Security contara con la validación de VMware Ready. Dentro de las iniciativas de virtualización de nuestra empresa, la implementación de un appliance virtual permitía reducir el coste total por propiedad y facilitaba la gestión en comparación con nuestra solución anterior basada en hardware.”

Mark L. Smith, Administrador de redes, Ochsner Health System

VII. PROTECCIÓN VIRTUAL EN EL GATEWAY PARA EL CORREO ELECTRÓNICO EN ENTORNOS VMWARE

En una situación de crisis económica, resulta más sensato que nunca implementar soluciones virtualizadas para la seguridad del correo electrónico en el gateway. El appliance virtual InterScan Messaging Security de Trend Micro permite obtener una protección galardonada de forma rápida y sencilla y aprovechar las ventajas en cuanto a disponibilidad, escalabilidad, continuidad del negocio y ahorro de costes inherentes a un entorno virtualizado VMware.

Para obtener más información, visite el punto de venta de appliances virtuales de VMware, en <http://www.vmware.com/appliances>, donde podrá conocer más datos sobre los appliances virtuales y descargar una copia de evaluación. Además, visite Trend Micro en www.trendmicro.com



VIRTUALIZACIÓN DE LA SEGURIDAD EN EL GATEWAY DEL CORREO ELECTRÓNICO

ACERCA DE VMWARE

VMware es el líder mundial en cuanto a soluciones de virtualización, desde el equipo de escritorio hasta Internet, pasando por el centro de datos. VMware proporciona los cimientos para más iniciativas de consolidación y virtualización de centros de datos que ninguna otra empresa. Entre sus clientes se cuentan más de 130 000 organizaciones de todos los tamaños pertenecientes a todos los sectores, incluidas todas las de la lista Fortune 100 y el 96% de Fortune 1000, así como PYMES.

ACERCA DE TREND MICRO

Trend Micro Incorporated, líder mundial en la seguridad de contenidos en Internet, centra su actividad en el intercambio de información digital para empresas y consumidores. Como empresa pionera y líder en el sector, Trend Micro adelanta una tecnología integrada para la gestión de amenazas a fin de proteger la continuidad de trabajo y la propiedad frente al malware, spam, filtraciones de datos y amenazas Web más recientes. Visite TrendWatch en www.trendmicro.com/go/trendwatch para obtener más información sobre las amenazas más recientes. Las flexibles soluciones de Trend Micro, disponibles en diversas configuraciones, cuentan con la asistencia técnica ininterrumpida de un equipo internacional de expertos en amenazas. Muchas de estas soluciones integran la tecnología Trend Micro Smart Protection Network, una infraestructura de última generación para la seguridad de contenidos de clientes por Internet que protege a los clientes frente a las amenazas Web. Trend Micro es una empresa transnacional con sede en Tokio y sus fiables soluciones de seguridad se venden a través de sus socios empresariales en todo el mundo.

©2009 by Trend Micro Incorporated. Reservados todos los derechos. Trend Micro, el logotipo en forma de balón de Trend Micro y TrendLabs son marcas registradas o marcas comerciales de Trend Micro Incorporated. El resto de los nombres de productos y empresas pueden ser marcas comerciales o marcas registradas de sus respectivos propietarios. La información del presente documento puede modificarse sin previo aviso. [WP01_VMWARE_0980730ES]