2011, el año en que cambió la seguridad

Alejandro Solana

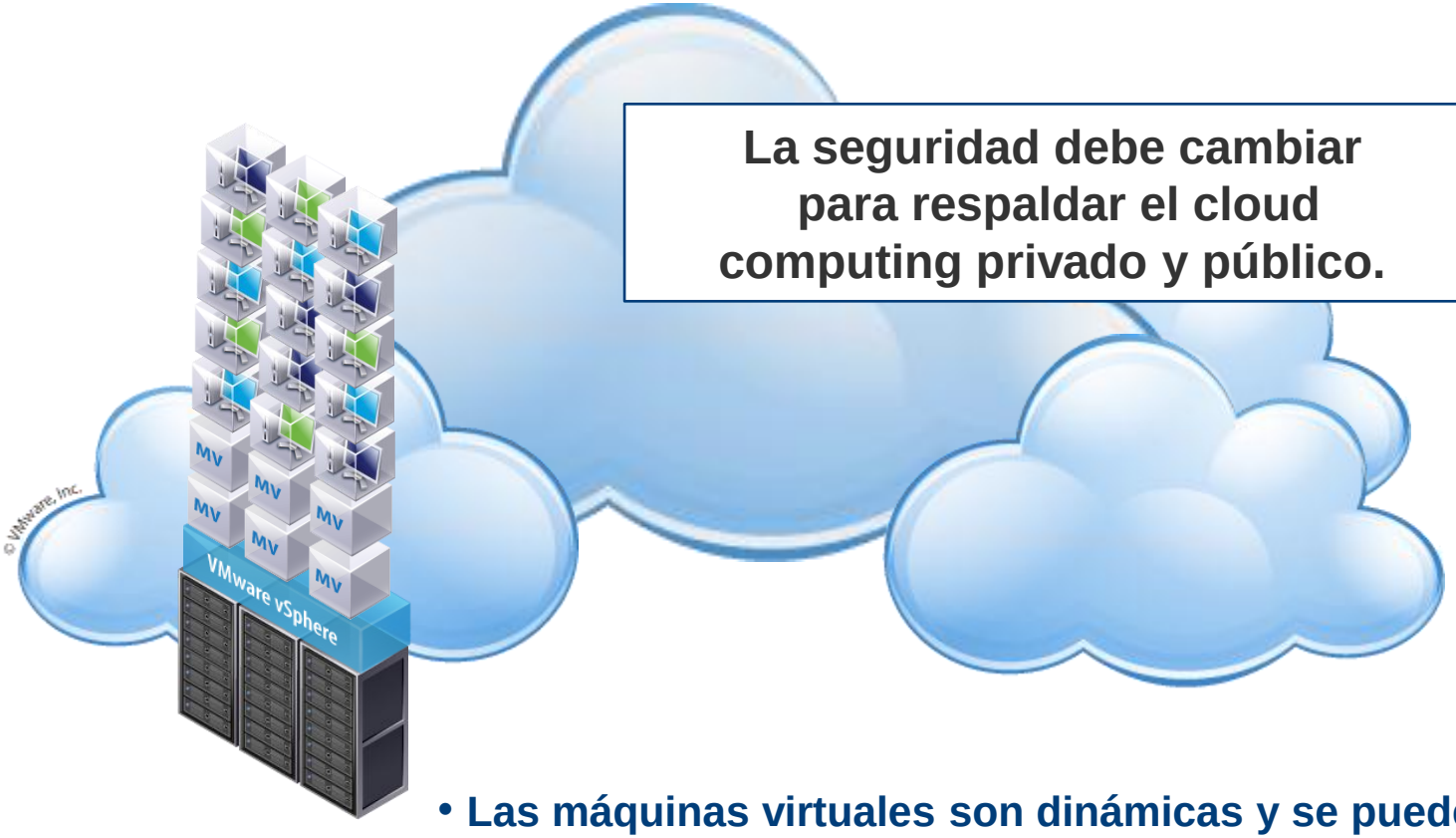
Iberia Presales Manager

La seguridad y el cumplimiento son las principales preocupaciones en lo que a la cloud se refiere

La virtualización constituye la base para la creación de clouds privadas. La seguridad debe cambiar para respaldar ambas cosas.

– Gartner, 2010

Nuevos desafíos derivados del cloud computing



- Las máquinas virtuales son dinámicas y se pueden mover de un lugar a otro.
- Las máquinas virtuales se crean con facilidad y puede autoaprovisionarlas personal que no pertenezca a TI.
- Aumento de las cargas de trabajo con gran cantidad de escritorios virtuales en el centro de datos.

Nuestra respuesta: seguridad diseñada para el cloud computing

VMware vShield habilita la seguridad

1. Introspección única
2. Abstracción de políticas

Rentable

- Un único dispositivo virtual con completas funcionalidades
- Un solo framework para protección exhaustiva

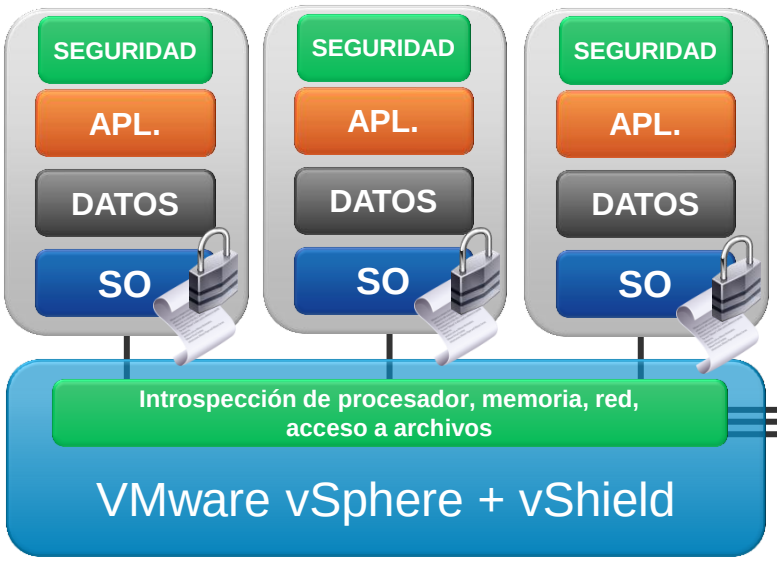
Fácil

- Sin proliferación de reglas, VLAN ni agentes
- Visibilidad pertinente para los administradores de la infraestructura virtual y los equipos de redes y de seguridad
- Cumplimiento simplificado

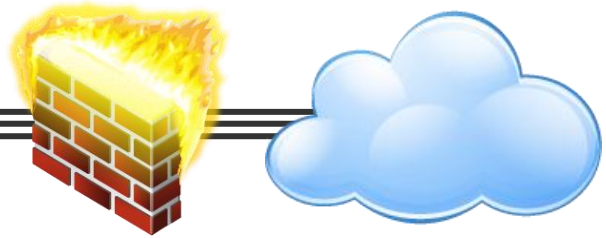
Adaptativo

- Con reconocimiento de virtualización y cambios
- Se programa una vez, se ejecuta en todas partes
- Solución rápida de problemas

Enfoque tradicional o vShield



Seguridad basada en host



Seguridad basada en red

- Pro
- Rec
- Ider
- Rec

age

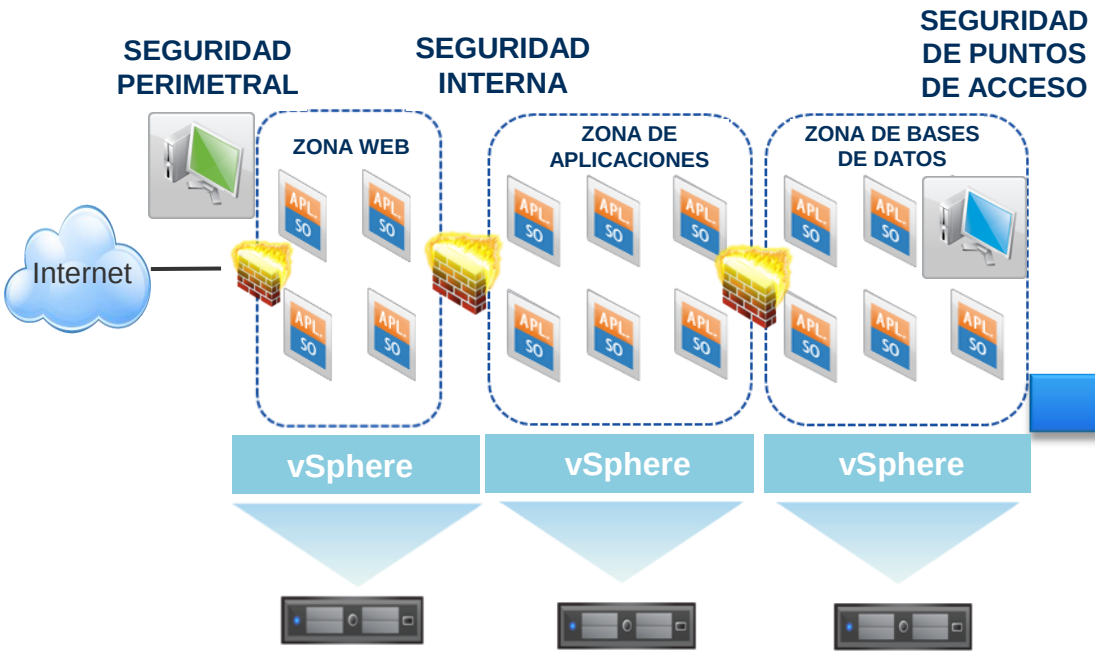
Ventajas

- Creación y aplicación de políticas de seguridad con migración en caliente, balanceo automático de la carga de las MV y reinicio automatizado de MV
- Aprovisionamiento rápido de políticas de seguridad
- Cumplimiento más fácil con seguimiento continuo y registro exhaustivo

Soluciones de seguridad de VMware

- **Seguridad perimetral**
- Protección de aplicaciones contra amenazas de la red
- Desafíos antivirus en entornos de virtualización y de cloud

Protección del centro de datos virtual (vDC) con soluciones de seguridad heredadas



- Pods aislados físicamente con hardware físico dedicado
- Clústeres de confianza mixtos, sin segmentación de seguridad interna
- Complejidad de la configuración
  - Proliferación de VLAN
  - Proliferación de reglas de firewall
  - Reglas IP de la red rígidas, sin contexto de recursos
- Clouds privadas (¿?)

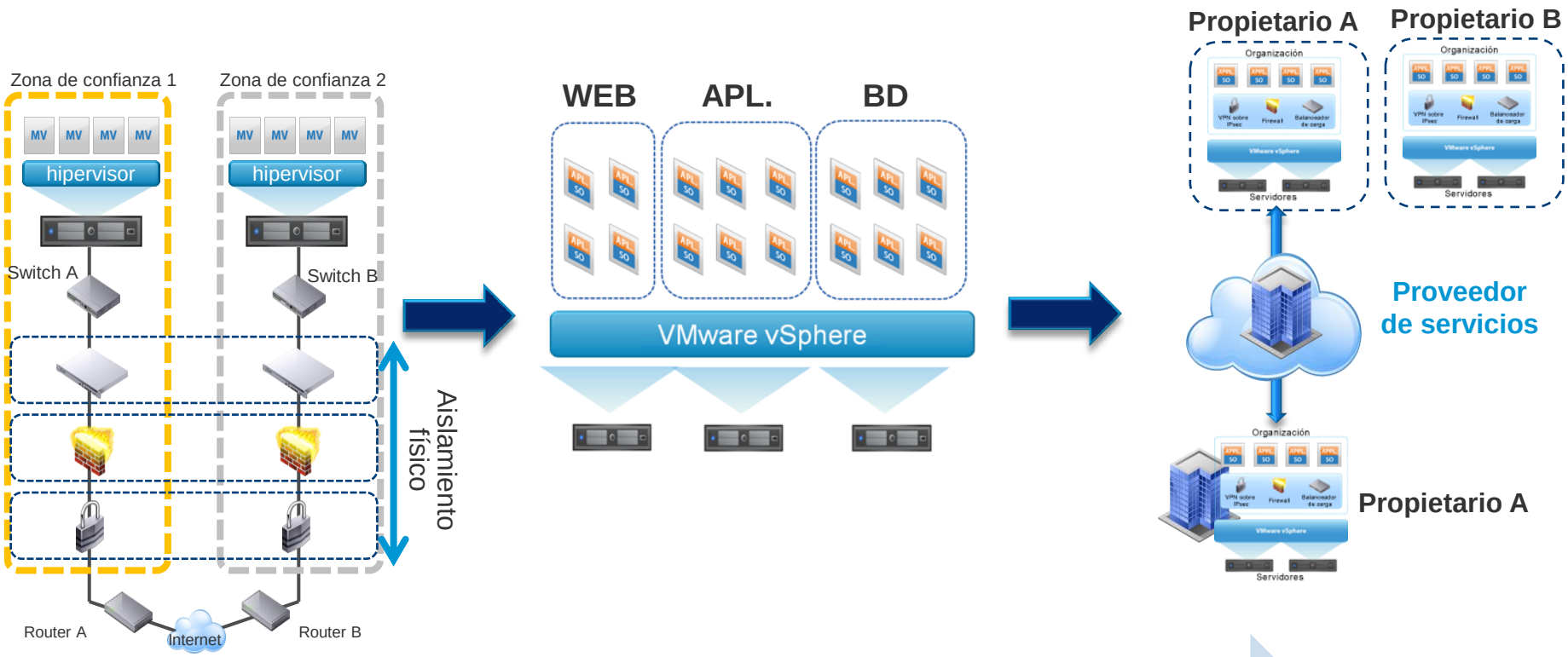
El cliente no puede hacer realidad las auténticas ventajas de la virtualización a causa de las preocupaciones de seguridad.

El método de seguridad tradicional consiste en el aislamiento físico

- Guía de seguridad de Otros Fabricantes:

  "Debe implementar las máquinas virtuales de forma que todas las MV de un equipo físico determinado compartan un nivel de confianza parecido".

Evolución de ls Seguridad hacia la cloud



Pods aislados físicamente

Zonas de confianza mixtas

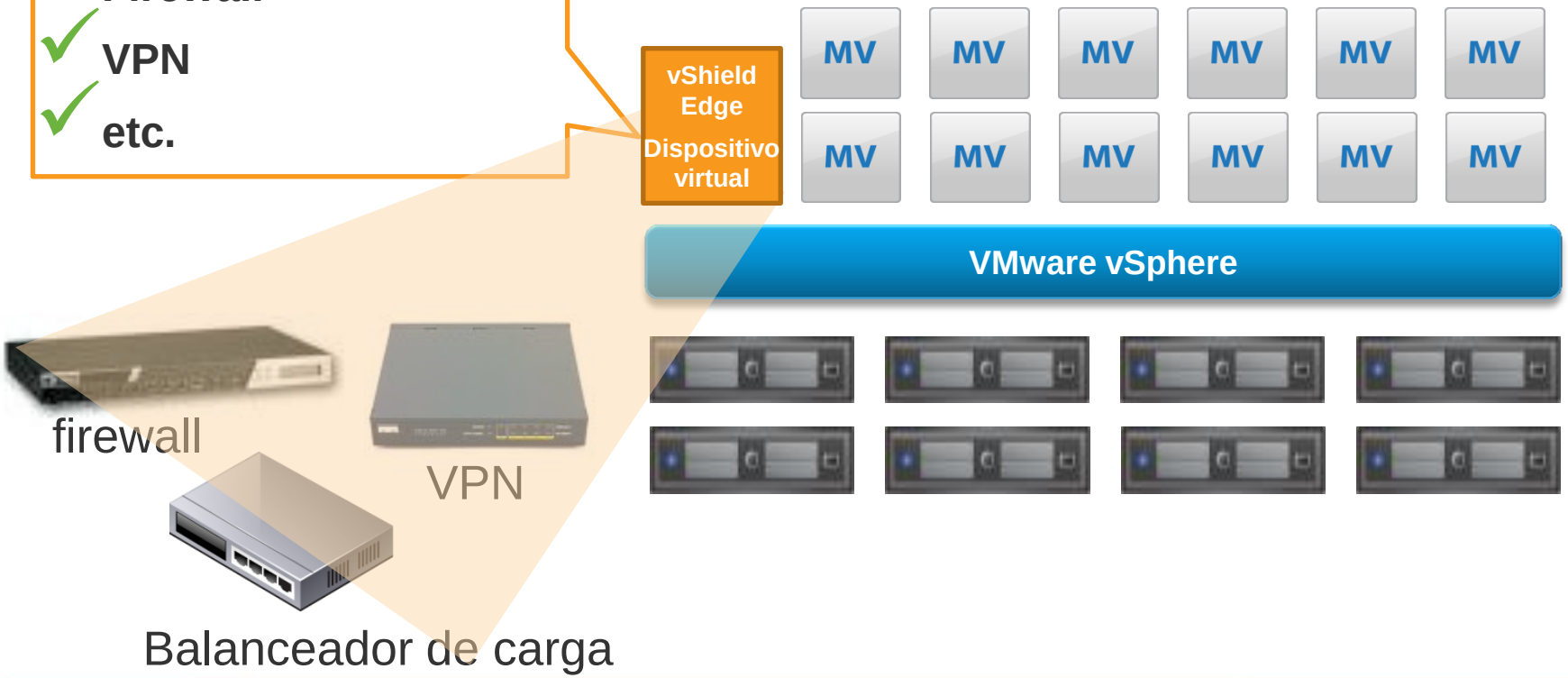
Clouds privadas

vmware

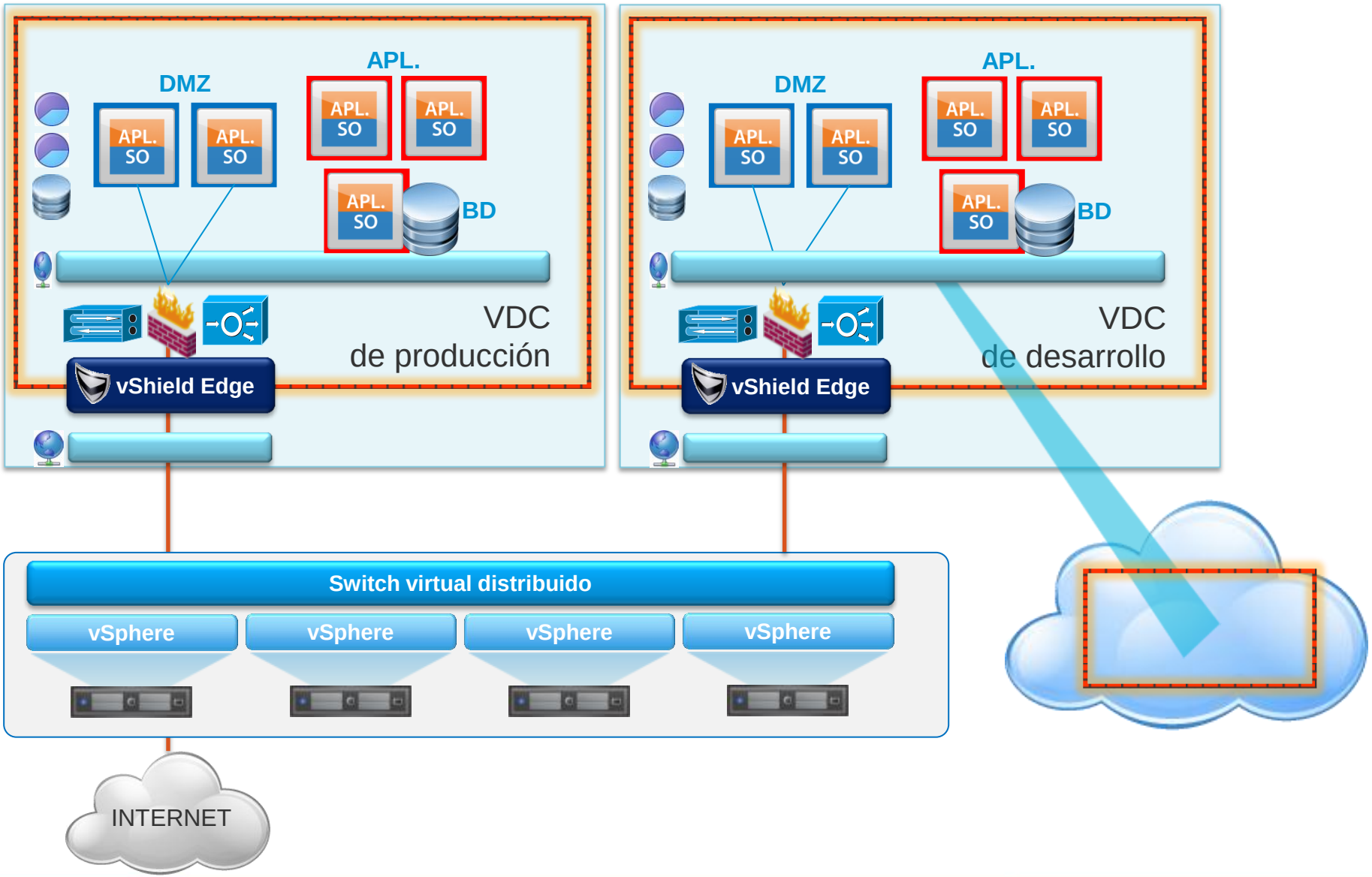
VMware transforma la seguridad cara en rentable

vShield elimina la necesidad de tener varios dispositivos de hardware específicos: multiplica por 3-5 el ahorro en gastos operativos y de capital

- ✓ Balanceador de carga
- ✓ Firewall
- ✓ VPN
- ✓ etc.



Seguridad perimetral automatizada de vCPD de cloud con vShield Edge



vShield Edge reduce el coste de la seguridad

Solución de seguridad perimetral de la red
(Firewall + VPN + Balanceador de carga)

Supuestos

- 100 MV por perímetro
- Costes de vSphere

Hace posible el cloud computing privado y público

Zonas de confianza mixtas, entornos duplicados, muchos usuarios en la misma infraestructura virtual compartida

Mbps = Megabits/segundo

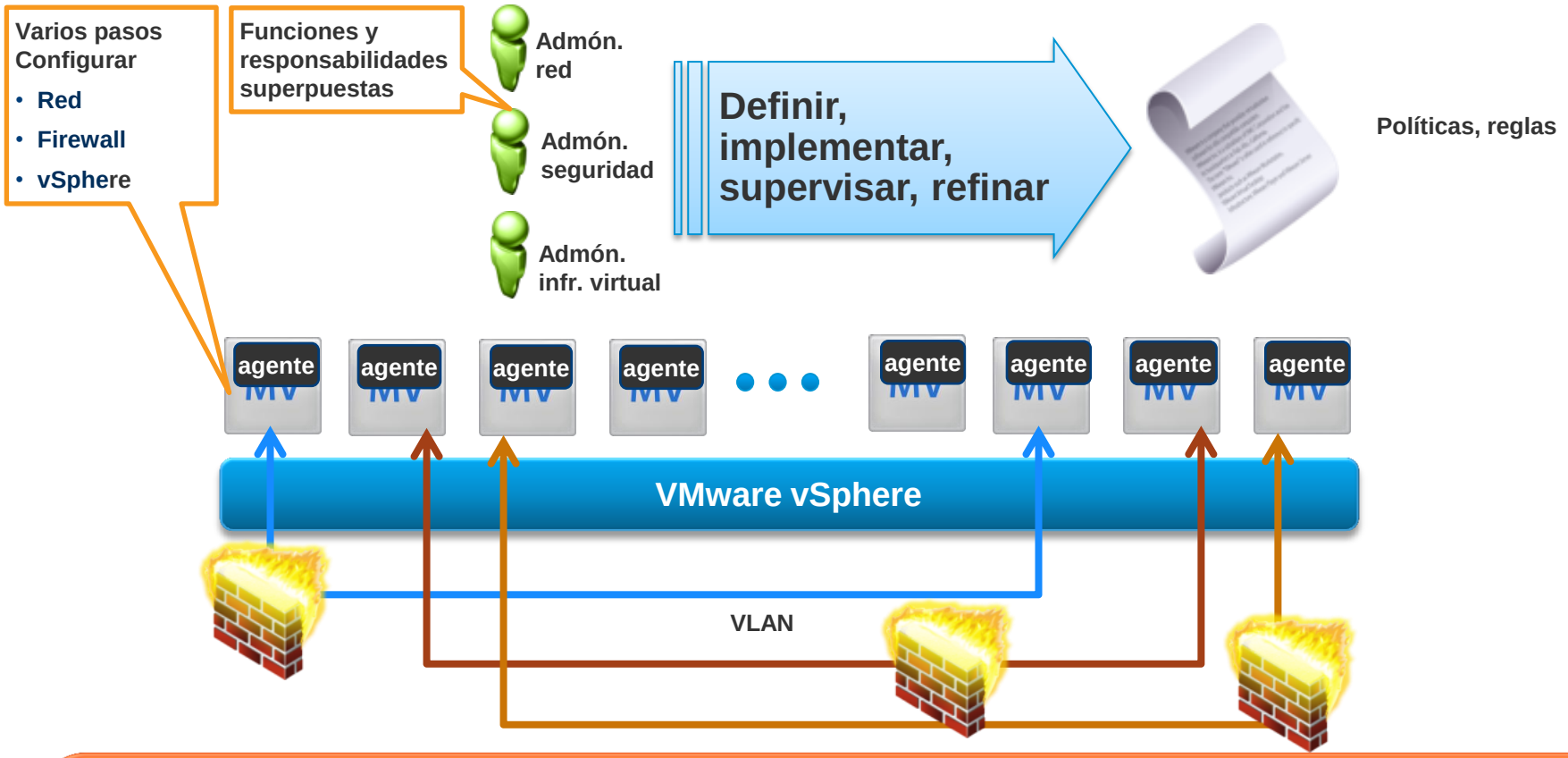
Gbps = Gigabits/segundo

vmware

Soluciones de seguridad de VMware

- Seguridad perimetral
- **Protección de aplicaciones contra amenazas de la red**
- Desafíos antivirus en entornos de virtualización y de cloud

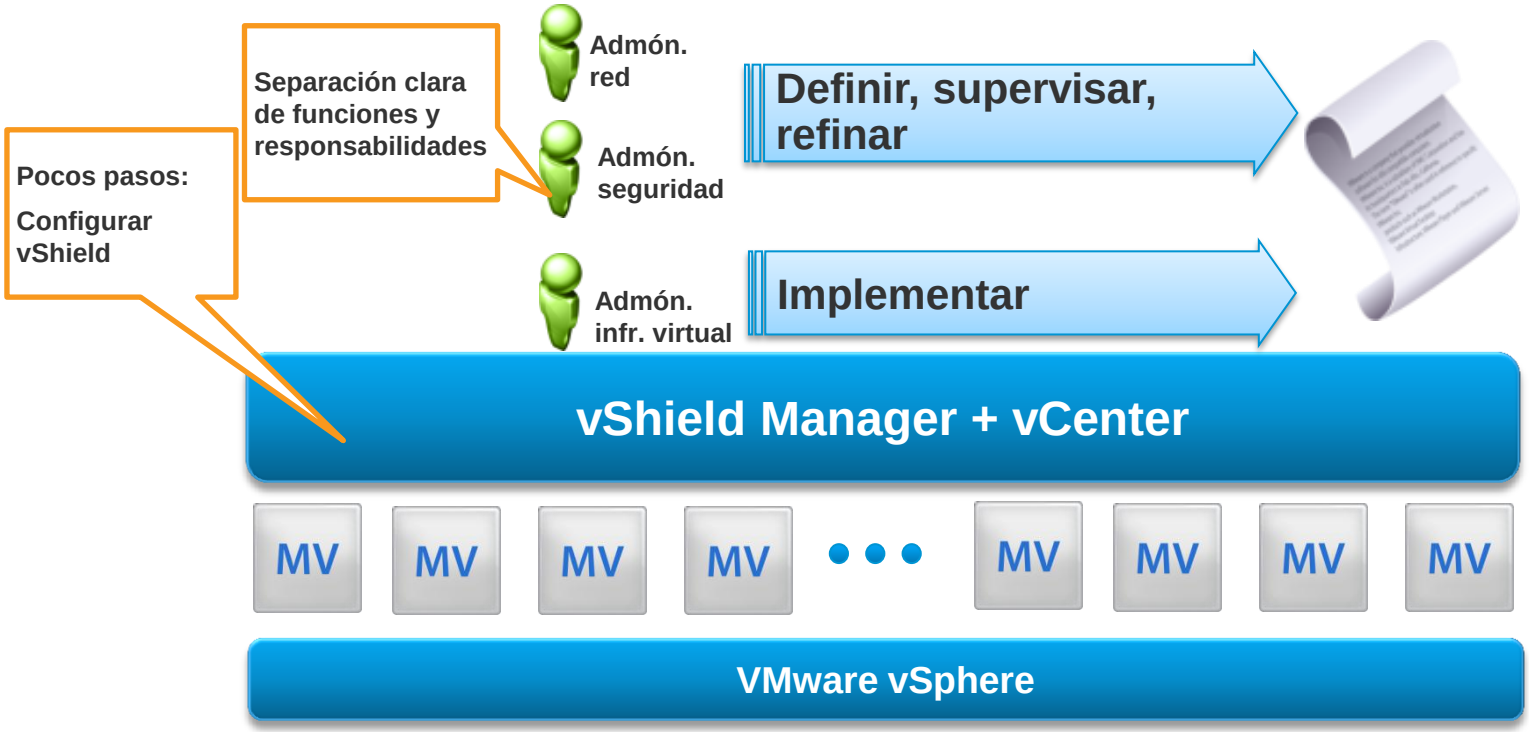
VMware transforma la seguridad compleja…



Complejidad

- Políticas, implementación de reglas: sin separación clara de obligaciones, confusión organizativa
- Varios pasos: configurar la red, el firewall y vSphere
- Sucesión y proliferación de VLAN: reglas de firewall, agentes

…en algo sumamente sencillo

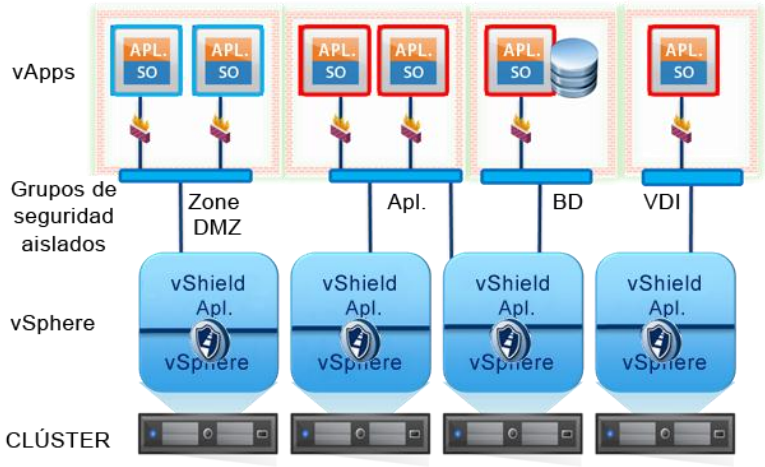


Fácil

- Separación clara de obligaciones
- Pocos pasos: configurar vShield
- Eliminación de proliferación de VLAN: firewalls vNIC
- Eliminación de reglas de firewall, proliferación de agentes
- Habilitación automática de seguridad en MV y apls. nuevas (auto) aprovisionadas

Protección de aplicaciones contra amenazas de la red

- Firewall de nivel de hipervisor
  - Control de conexión de entrada y salida aplicado en el nivel de vNIC
- Grupos de seguridad elásticos: se “estiran” a medida que se migran máquinas virtuales a otros hosts
- Supervisión de flujos robusta
- Gestión de políticas
  - Políticas simples y pertinentes para la empresa
  - Gestión desde la interfaz de usuario o API REST
- Registro y auditoría basados en el formato syslog estándar del sector



Aprovechamiento de la virtualización para lograr una seguridad mejor que la física

- **Principales ventajas**
  - Visibilidad y control completos del tráfico entre las MV, que permite la coexistencia de varias zonas de confianza en el mismo clúster ESX
  - Política de lenguaje empresarial intuitiva que aprovecha el inventario de vCenter
  - Habilitación del aprovisionamiento de autoservicio al aplicar políticas de seguridad en las MV o aplicaciones

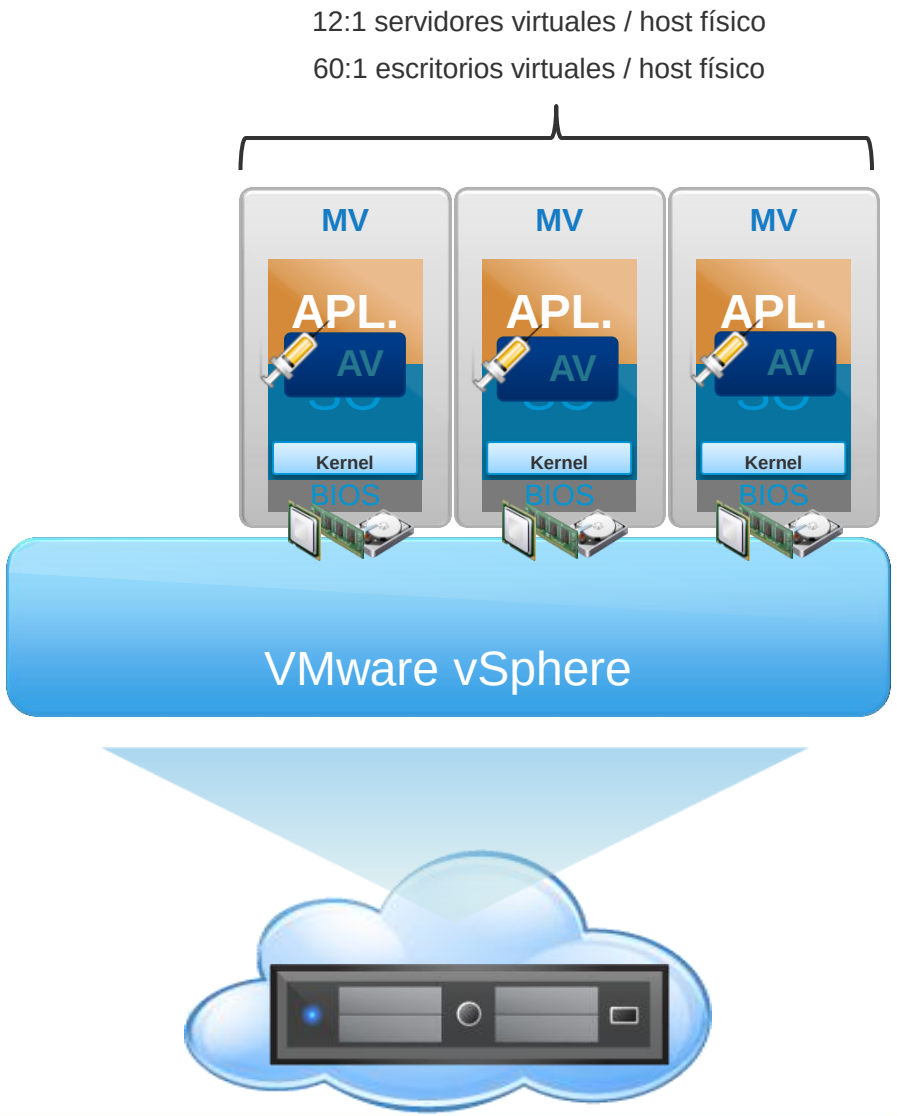
- **Mejor que la opción física**
  - Firewall virtual con densidad de puertos ilimitada
  - Introspección de nivel de hipervisor que proporciona acceso al tráfico entre las MV
  - Independiente de la topología sin tener en cuenta la configuración de la red, porque las políticas siguen las políticas de las MV que son independientes de la dirección IP
  - Las capacidades de firewall incorporadas proporcionan una seguridad mejor que la física por una tercera parte del coste

Soluciones de seguridad de VMware

- Seguridad perimetral
- Protección de aplicaciones contra amenazas de la red
- **Desafíos antivirus en entornos de virtualización y de cloud**

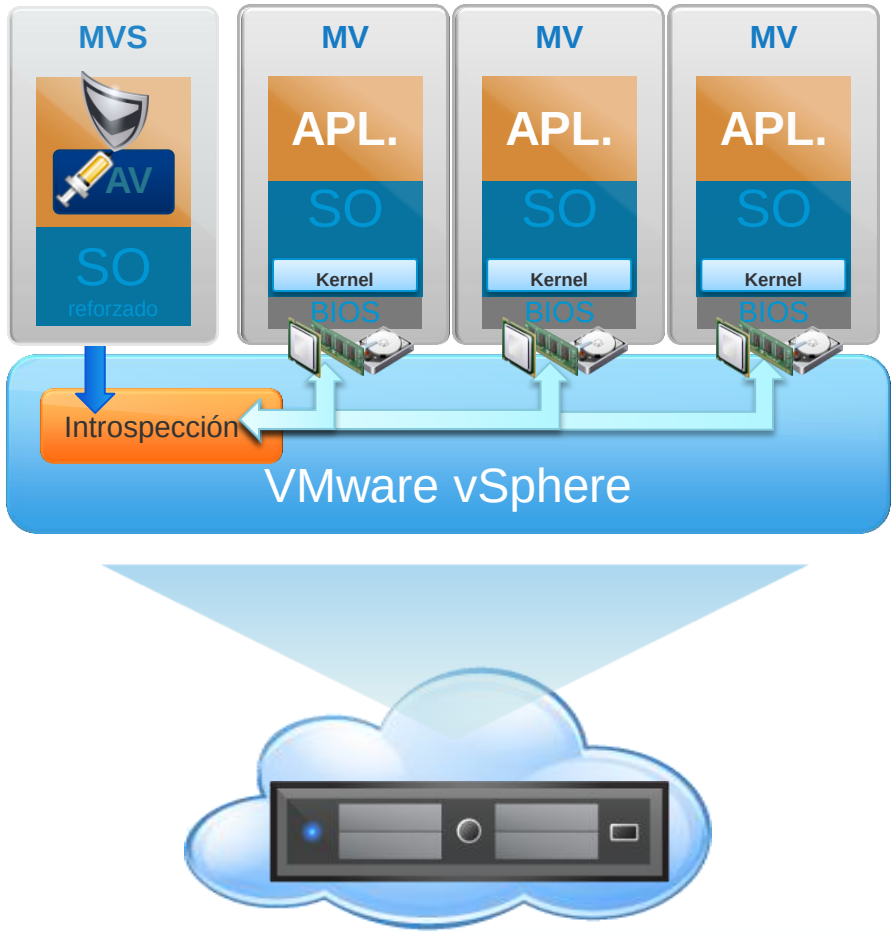
Desafíos antivirus en la virtualización y la cloud

- **Problemas**
  - Las “incidencias de AV” pueden provocar interrupciones del servicio en los entornos de informática (virtualización) y almacenamiento (SAN/NAS) compartidos.
  - Los agentes tradicionales utilizan los recursos de forma intensiva, no están optimizados para clouds eficaces de alto nivel de utilización.
    - Hasta 6 GB en escritorios VMware View.



Aprovechamiento de la virtualización para lograr una seguridad mejor que la física

- **Problemas**
  - Las “incidencias de AV” pueden provocar un 100% de saturación en los entornos informáticos (CPU) y de SAN/NAS (E/S de almacenamiento) compartidos.
  - Los agentes tradicionales utilizan los recursos de forma intensiva, no están optimizados para clouds eficaces de alto nivel de utilización.
    - Hasta 6 GB en escritorios VMware View.
- **Oportunidades**
  - Aprovechar el hipervisor para descargar las funciones de AV de los agentes y trasladarlas a una MV específica dedicada a la seguridad.
  - Implementar la seguridad de una forma más ágil y basada en servicios, en los entornos de cloud privada y pública.



Antivirus como servicio eficaz para centros de datos virtuales

- **Esfuerzo de colaboración más estrecha con los principales partners de AV**
- **Introspección basada en hipervisor para las principales funciones de AV**
  - La carga de los motores de análisis de archivos y las definiciones de virus se trasladan a la MV de seguridad, de forma programada y en tiempo real.
  - Controlador de virtualización de archivos ligero en el guest: más del 95% de reducción de la huella de guests (que con el tiempo llega a no necesitar ningún agente).
- **Implementable como servicio**
  - Sin agentes que gestionar.
  - Prestación llave en mano, de seguridad como servicio.
- **Aplicable a todos los modelos de implementación de la virtualización:**

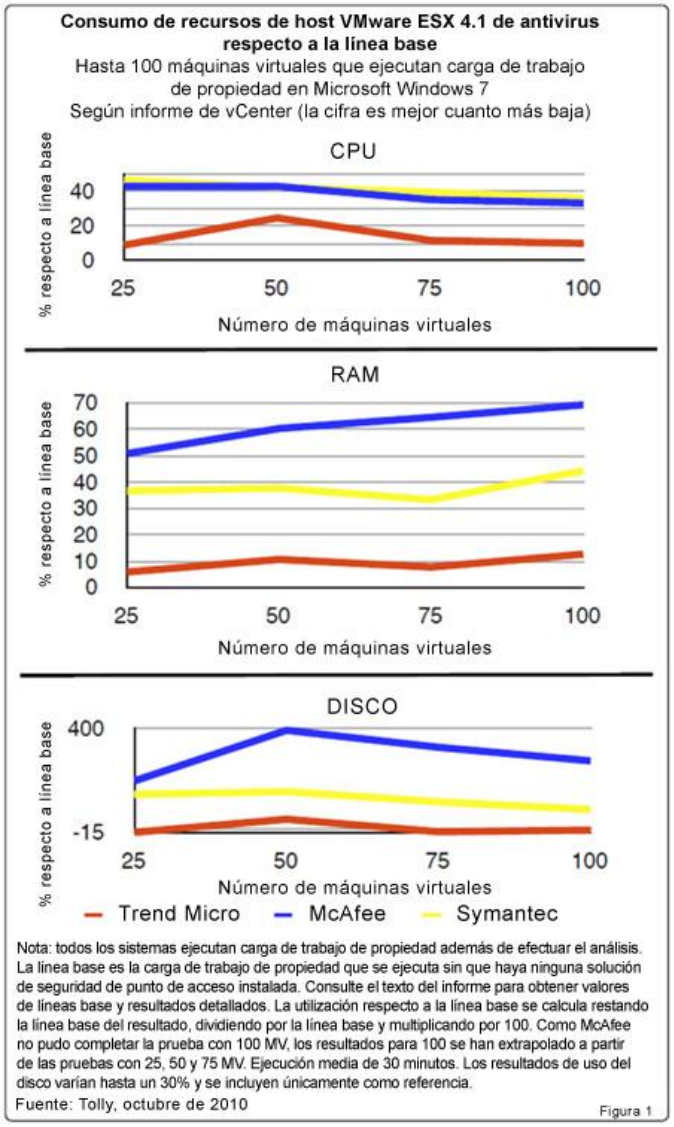
  clouds privadas (centros de datos privados),

  clouds públicas (proveedores de servicios),

  escritorios virtuales.

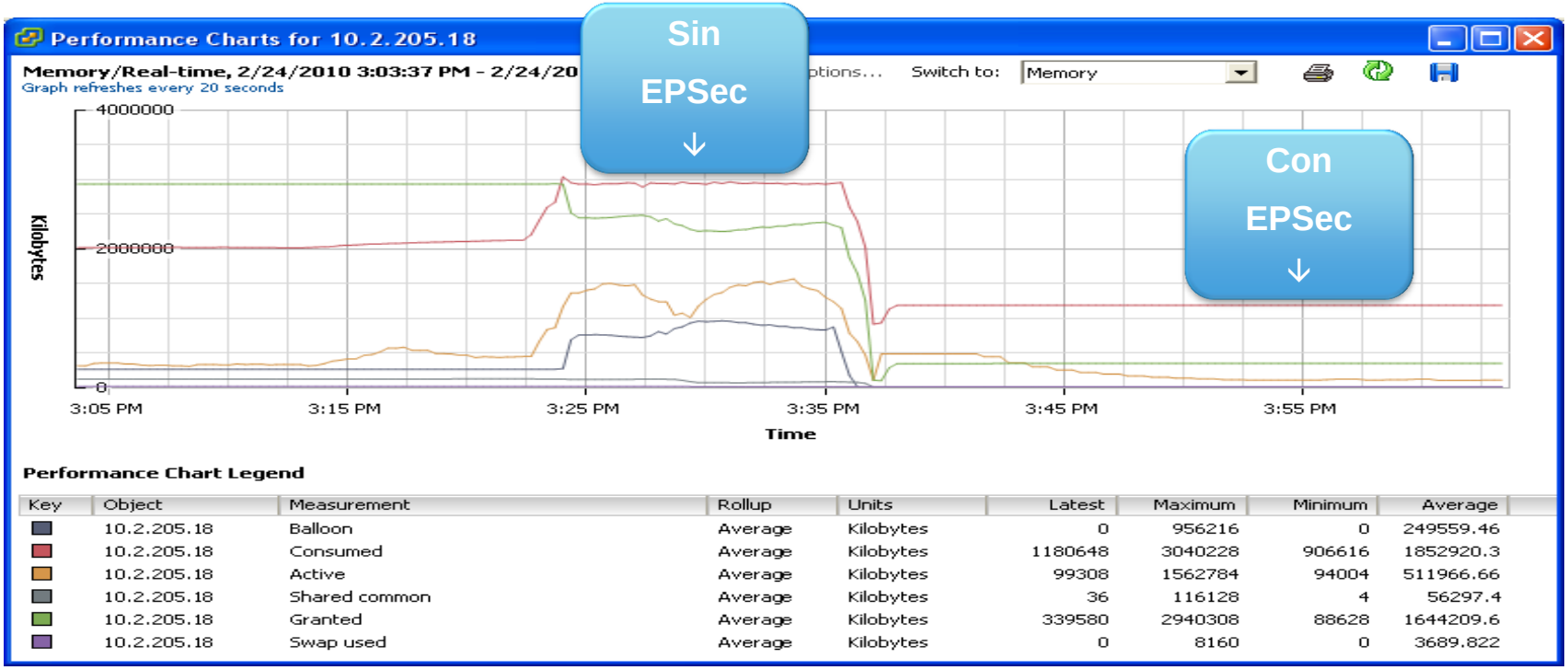
Consumo eficaz de los recursos

- **Enfoque de servidor de análisis significa:**
  - Sin huella de agentes
  - Menos sobrecarga de memoria y gestión
  - Menos carga de CPU y E/S



Utilización eficaz de la memoria

El enfoque de servidor de análisis significa que no se necesita huella de agentes, y menos sobrecarga de memoria y de gestión



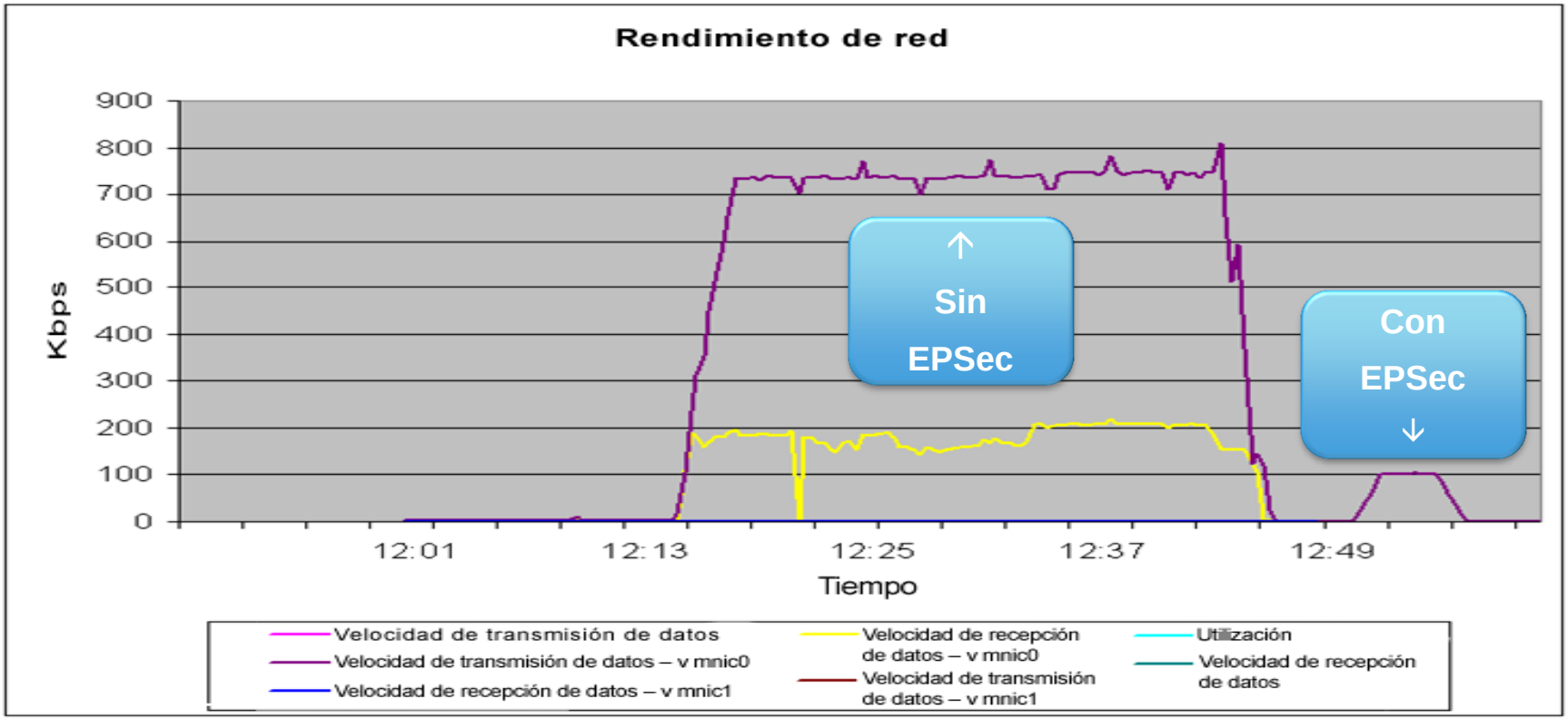
Key	Object	Measurement	Rollup	Units	Latest	Maximum	Minimum	Average
	10.2.205.18	Balloon	Average	Kilobytes	0	956216	0	249559.46
	10.2.205.18	Consumed	Average	Kilobytes	1180648	3040228	906616	1852920.3
	10.2.205.18	Active	Average	Kilobytes	99308	1562784	94004	511966.66
	10.2.205.18	Shared common	Average	Kilobytes	36	116128	4	56297.4
	10.2.205.18	Granted	Average	Kilobytes	339580	2940308	88628	1644209.6
	10.2.205.18	Swap used	Average	Kilobytes	0	8160	0	3689.822

ANTES: enfoque tradicional basado en agentes

DESPUÉS: dispositivo virtual de seguridad que usa Vmware End Point Security (EPSec)

Ancho de banda eficaz de E/S

Ancho de banda durante la actualización de definiciones de virus



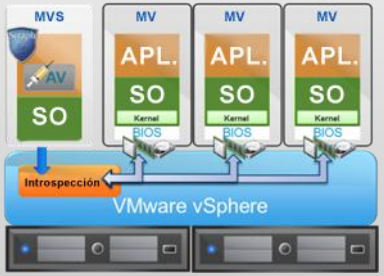
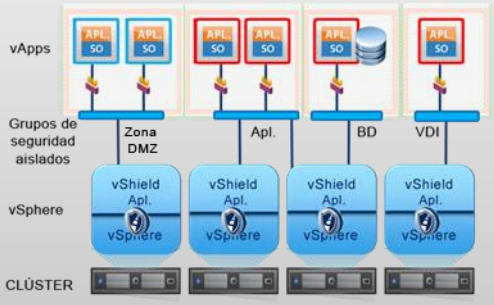
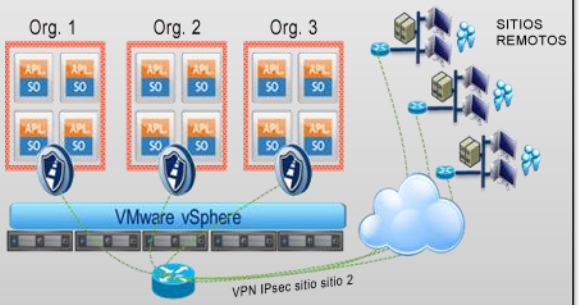
ANTES: enfoque tradicional basado en agentes

DESPUÉS: dispositivo virtual de seguridad que usa Vmware End Point Security (EPSec)

Resumen de soluciones antivirus disponibles basadas en vShield End Point

Disponible	Producto
Hoy	Trend Micro Deep Security 7.5
Más adelante en 2011	KASPERSKY lab symantec.
Por confirmar	McAfee

VMware: habilitamos la seguridad para la cloud

Dentro de la MV	MV <-> red	Perímetro vCloud/VDC
		
vShield Endpoint	vShield App	vShield Edge

- **Primeros del sector en las tres áreas**
- **Simplificación y automatización radicales**
- **Posicionados para unificar la administración de políticas de seguridad**

La solución idónea para su proyecto

Virtualización del centro de datos	Cloud computing privado/público	Informática para el usuario/Virtualización de escritorios *
• vShield App	• vShield Edge • vShield App	• vShield End Point * • vShield App

PREGUNTAS Y RESPUESTAS

* vShield End Point se incluye con VMware View Premier.

2011, el año en que cambió la seguridad

Alejandro Solana

Iberia Presales Manager