PowerGate: un sistema de seguridad, alta disponibilidad y gestión de ancho de banda basado en GNU/Linux

Javier Miguel Rodriguez

Optima Technologies

javier.miguel@optimat.com

Optima Technologies es una organización con sede en Sevilla y cuyo ámbito de influencia se extiende por la Comunidad Autónoma de Andalucía. Fue fundada en Febrero de 1996 con el objetivo de competir en el sector de las TI ofreciendo a las empresas una elevada solvencia tecnológica en integración de Sistemas y Soluciones a un precio altamente competitivo, considerando sus competidores naturales a organizaciones cuya estructura de costes es mucho más pesada y se ven obligadas a trasladar esos costes a sus clientes.

Resulta evidente para Optima la necesidad de la especialización, con una infraestructura relativamente liviana en costes (y recursos) resulta imprescindible determinar las áreas de competencia tecnológica y hacer foco en ellas a través de los programas de formación y reciclaje además de las inversiones en productos, documentación y equipamiento.

Nuestra primera opción como plataforma tecnológica fueron los Sistemas de Digital Equipment, que nos permitía ofrecer a los clientes el superior rendimiento y fiabilidad de las plataformas RISC Alpha con Digital Unix.

Pero nuestra visión de la solución en la empresa es siempre la constatación de que los entornos son, de forma natural, heterogéneos,

por lo que resultaba necesario incorporar la oferta de plataformas heterogéneas en las áreas de ofimática y redes, la evolución del mercado nos apuntó claramente a adoptar en estas áreas las soluciones de Microsoft, el tiempo nos ha dado la razón en esta elección.

Nuestra vocación es ofrecer soluciones globales, por lo que incorporamos a nuestro catálogo de productos y servicios las soluciones de almacenamiento StorageWorks basadas en fibrechannel y el desarrollo de soluciones Intranet para la colaboración en entornos corporativos.

Linux ha sido nuestra ultima adopción tecnológica al ser uno de los fenómenos de mayor relevancia en el mercado de TI, pero nuestro enfoque no puede ser "sólo Linux". Somos integradores y como tales, insistimos en que de forma natural las soluciones han de coexistir en entornos heterogéneos (¿para qué existen los estándares y la interoperabilidad si no nos permiten obtener lo mejor de cada entorno?).

Sabemos que Linux es un sistema con un tremendo potencial y por ello hemos apostado por la plataforma invirtiendo recursos en I+D de soluciones que, de forma natural, se integren en entornos heterogéneos. Es un modo de proteger la inversión de los clientes a la vez que facilitamos la entrada de Linux como solución plenamente aceptada en la comunidad de responsables de TI de las empresas.

Para nosotros la visión "sólo Linux" tiene hoy día un escaso impacto. Es lo mismo que la visión "todo Solaris" de Sun o cualquier otro sabor de una proyección sobre un solo entorno. Ciertamente no conocemos demasiados casos y de cualquier modo chocan frontalmente con lo que entendemos que es beneficioso para el cliente.

Nuestra visión es lo que nos ha permitido tener un gran éxito comercial, nuestra facturación ha crecido desde los 30 millones de 1996 a los 500 millones del año 2000, lo que avala nuestra política y su aceptación entre nuestro mercado-objetivo.

1. ¿Qué es PowerGate?

PowerGate es una solución integral para el control de acceso a redes corporativas. Está basado en GNU/Linux RedHat 6.2 y kernel 2.2.19, por tratarse de la distribución y versión de kernel certificados por el fabricante del hardware, Compaq. PowerGate se migrará a kernel 2.4.x cuando esta rama del kernel haya alcanzado la estabilidad suficiente y Compaq certifique una distribución con kernel 2.4.x.

La principal ventaja de PowerGate es su integración. Unir en una misma máquina funcionalidades tan variadas como cortafuegos, proxy, calidad de servicio, red privada virtual, detección de intrusos y alta disponibilidad hacen de él un producto atractivo para la pequeña y mediana empresa, pues ofrece un nivel de protección razonable a un precio muy competitivo.

PowerGate se comercializa como un producto empaquetado, incluyendo la plataforma software y el hardware. El hardware está basado en los robustos servidores Intel de la gama Proliant de Compaq o en los potentes servidores Alpha de 64 bits.

2. Funcionalidades de PowerGate

2.1. Cortafuegos

El cortafuegos es un elemento clave en cualquier red corporativa, su labor es mantener al mínimo necesario los puntos de contacto entre el tráfico de red interno y externo. Un cortafuegos NO es una solución completa de seguridad, es tan solo parte de una buena política, pues permite delimitar que tráfico debe fluir desde Internet a nuestra red y viceversa.

PowerGate utiliza *ipchains* para realizar las funciones de cortafuegos. Permite realizar conexiones compartidas a Internet usando la técnica de *masquerading,* algo muy útil en conexiones a Internet con tecnologías Frame Relays, cable y ADSL. Con unas buenas reglas de filtrado se puede conseguir un nivel de seguridad razonable, adecuando las conexiones de red a la política de seguridad de la empresa.

2.2. Monitor de tráfico de red / QoS

El ancho de banda corporativo es un bien escaso y caro. Se debe realizar un control exhaustivo sobre él para evitar abusos y a su vez garantizar un ancho de banda suficiente para las necesidades corporativas (tales como servidores de correo, web, etc)

Para poder establecer una buena política de uso de ancho de banda se ha de poder realizar un seguimiento del uso del ancho de banda. PowerGate provee un historial detallado del uso de la red, permitiendo establecerse con estos datos una política de consumo del ancho de banda basada en argumentos reales, no suposiciones de consumo.

Una vez que tenemos claro el consumo del ancho de banda, se dispone de una herramienta para ajustar el consumo del ancho de banda de acuerdo a parámetros tales como IP fuente, IP destino, puertos fuente/destino y hora del día.

PowerGate emplea *iproute* y *tc* junto con técnicas de *cbq* para controlar el uso del ancho de banda corporativo.

2.3. Proxy (transparente o no)

Un proxy es un software de centralización y control de un protocolo de red determinado. Los clientes, en vez de conectarse directamente a la ubicación remota, lo hacen a través del servicio de proxy. Así, un proxy web hace que toda conexión HTTP de un cliente pase por él antes de llegar a un servidor remoto. Las principales ventajas de un proxy son:

1. El proxy es el único realmente conectado a Internet, aumentando la seguridad
2. Se puede hacer un control efectivo de contenidos, al ser un software especializado
3. Es una buena manera de acelerar la conexión a Internet mediante técnicas de cacheo

Como software de proxy PowerGate emplea *squid*, pues ha demostrado su enorme potencia y flexibilidad como proxy (transparente o no), permitiendo un adecuado control de contenidos así como una efectiva aceleración de la navegación web.

2.4. VPN

VPN es el acrónimo de *Virtual Private Network*, red privada virtual. Podríamos definir una VPN como una red privada (y por tanto confiable) construida usando infraestructura pública (y por tanto no confiable). El principal uso que se les da a las VPN es la interconexión de redes privadas de delegaciones alejadas geográficamente usando como medio Internet, en vez de usar líneas dedicadas para ello, siendo por tanto un ahorro respecto a una infraestructura propia de telecomunicaciones. Otro posible uso es la realización de teletrabajo de una manera segura.

Por tanto, una VPN aporta privacidad, un ahorro de costes de mantenimiento y un ahorro de costes en infraestructuras, pues cualquier persona autorizada podrá trabajar como si estuviera en la oficina, aunque geográficamente puede estar en cualquier parte . Las principal desventaja es un mayor consumo del ancho de banda corporativo.

Una VPN usa diferentes técnicas de encriptación y seguridad para garantizar que sólo usuarios autorizados puedan acceder a la red y que los datos no puedan ser interceptados.

PowerGate se basa en el estándar abierto *IPSEC* y en su implementación libre, *freeswan* para realizar VPNs.

2.5. IDS y análisis de logs

Una buena política de seguridad ha de tener muy en cuenta el análisis de logs y el uso de IDS (Intrusion Detection System) para detectar intrusiones; ninguna herramienta de seguridad es perfecta, por lo que alguna intrusión puede llegar a tener éxito. Es por ello que semejante contingencia ha de ser detectada lo antes posible para que el daño realizado sea mínimo.

PowerGate contempla esta eventualidad facilitando el análisis de logs y con la capacidad de que el administrador defina situaciones potencialmente sospechosas ante la cual PowerGate reacciona generando alertas tales como correos electrónicos, mensajes a móviles o avisos a máquinas en red. Powergate emplea para ello la capacidad de logueo de todos sus componentes así como *logcheck* para definir políticas de avisos.

A su vez, PowerGate cuenta con la posibilidad de generar "respuestas automáticas" ante determinados eventos sospechosos. Un ejemplo claro es añadir automáticamente una regla de cortafuegos ante repetidos escaneos de puertos desde la misma IP. De cualquier manera, esto ha de ser evaluado y considerado por el administrador, que es el encargado de definir que es sospechoso o no.

2.6. Alta disponibilidad

En determinados ambientes corporativos la conexión a Internet es un recurso crítico: un fallo hardware NO puede dejar sin conexión a Internet a la empresa. Es por ello por lo que PowerGate pueda ser configurado en alta disponibilidad en dos o más nodos, de tal modo que si uno de los nodos falla, el otro toma su función a los pocos segundos.

Para ello cada nodo comparte su configuración empleando software como *rsync* y *openssh*. La alta disponibilidad se consigue empleando técnicas de *heartbeat*para conseguir un failover de servicios en caso de fallo hardware.

PowerGate también soporta raid por hardware, para evitar que el fallo de un disco duro pueda degradar la conexión a Internet.

2.7. Facilidad de configuración

La principal "pega" que una empresa pone al uso de GNU/Linux es la dificultad de configuración. Un cortafuegos con tantas funcionalidades como PowerGate ha de ser un producto complejo, pues fusiona muchas tecnologías

Se ha puesto un especial hincapié en la facilidad de uso. Para ello se dispone de un interfaz de configuración web ssl que permite un sencillo control de todas las funcionalidades del PowerGate. Se han empleado fragmentos de *webmin* para la configuración de algunos servicios, siendo el resto desarrollo propio de Optima Technologies.

2.8. La competencia

PowerGate NO es un producto de gama alta. No es el mejor cortafuegos del mercado, ni el mejor proxy, ni el mejor gestor ancho de banda...no destaca en nada en especial, excepto en dos cosas:

1. *Es capaz de solucionar de forma satisfactoria muchos problemas de conectividad y seguridad de una empresa.* La mayor parte de las empresas NO necesitan todas las funcionalidades que dan productos como Checkpoint Firewall-1 o Raptor Firewall, pues sus necesidades no son tan complejas. PowerGate es capaz de cubrir perfectamente estas necesidades medias.
2. *La relación calidad/precio de PowerGate es superior.* En PowerGate el precio es un valor vital. Muchas empresas no pueden permitirse gastarse millones de pesetas en diferentes productos para tener una funcionalidad comparable a la de PowerGate

A su vez, PowerGate está dirigido a un segmento de mercado, el de las Medianas y grandes empresas no ISPs, en el que la problemática de la seguridad de redes está practicamente sin cubrir

2.9. Plan de futuro

PowerGate es un producto en continua evolución. Estas son las futuras líneas de investigación de PowerGate

1. Migración a kernel 2.4.x e iptables
2. Mejoras en el soporte de IDS con *snort* y *portsentry*
3. Integración en redes heterogéneas empleando *openldap*
4. Balanceo de carga por interfaces empleando las nuevas características de *tc* y *EQL*
5. Soporte de Itanium y mejor soporte de máquinas multiprocesador
6. Inclusión de pasarela de correo *qmail*
7. Inclusión de antivirus *avp*

Todo esto hace que PowerGate sea un producto vivo, pues la seguridad informática es un campo en continua evolución, no teniendo por tanto cabida las soluciones estáticas.

3. Ventajas de GNU/Linux

3.1. Flexibilidad y capacidad de adaptación del código abierto

Una de las principales ventajas del código abierto es su gran capacidad de adaptación. A nivel de kernel éste se puede optimizar para que de un mayor rendimiento como sistema de red. A su vez, las utilidades del sistema operativo pueden ser recompiladas para hacer un mejor uso del procesador, y se pueden eliminar servicios innecesarios para aumentar el rendimiento.

A su vez, tener una gran comunidad de desarrolladores de GNU/Linux es una garantía de seguridad de que GNU/Linux seguirá expandiéndose y convirtiéndose cada día en una plataforma más potente.

3.2. Estándares abiertos

PowerGate se basa por completo en estándares abiertos para garantizar la

interoperabilidad entre plataformas. *TCP/IP*, *ipsec* y *ssl* son los principales estándares abiertos que soporta PowerGate.

3.3. Seguridad a través de la calidad (y no oscuridad)

Todo software de seguridad ha de poseer el código fuente disponible. Es la única manera de garantizar la calidad de dicho software, cuando miles de ojos pueden revisarlo en busca de fallos. La seguridad a través de la oscuridad NO es seguridad.

Es por ello que todos los componentes de PowerGate son de código abierto.

3.4. Multiplataforma, escalabilidad y fiabilidad

PowerGate corre actualmente sobre plataformas Intel y Alpha. Pero es fácilmente portable a plataformas tales como Sparc o Itanium. Esta misma portabilidad garantiza una gran escalabilidad, pues se puede ejecutar sobre baratas máquinas Intel o sobre potentes servidores de 64 bits Alpha.

La fiabilidad demostrada por GNU/Linux es elevada, siendo una plataforma suficientemente estable como para encomendarle aplicaciones críticas. Se está avanzando a pasos agigantados en el aspecto de la alta disponibilidad, con diferentes implementaciones de tecnologías de cluster failover

3.5. Mayor rendimiento

GNU/Linux es, junto con FreeBSD, el sistema operativo de red que más rendimiento ofrece sobre plataformas Intel y Alpha. La capacidad de optimizar el núcleo y los servicios de red hacen que el sistema se comporte casi como un sistema embebido, con un rendimiento muy elevado.

3.6. Coste

Es innegable que el uso de GNU/Linux supone un enorme ahorro de costes respecto a otros sistemas operativos propietarios. Esto puede llegar a convertir a GNU/Linux en un producto de gran interés comercial para determinadas empresas