

# TCN

SUPLEMENTO DEL N° 280

CISCO SYSTEMS



# seguridad

de principio a fin



poweredbycisco.  
**sinlímites**

Puestos de trabajo en forma de espacios abiertos.  
Despachos despejados. No importa donde desee encontrar  
inspiración las redes de autodefensa de Cisco Systems le permiten  
acceder a la oficina a cualquier hora y desde cualquier lugar.  
Bienvenido a los negocios sin fronteras. Conozca como Cisco está  
ayudando a cambiar los negocios en  
[www.cisco.com/poweredby](http://www.cisco.com/poweredby)



seguridad. powered by



# Cisco hace realidad la autodefensa de las redes



**Yolanda Lamilla,**  
*directora de desarrollo de negocio de Cisco Systems en España*

Los directores de comunicaciones e informática de todo el mundo siguen dando máxima prioridad a la seguridad en la red. Merrill Lynch realizó un estudio en junio de 2005 en el que se preguntaba a directores de comunicaciones e informática, de los cuales el 40% eran europeos, en qué áreas iban a invertir su presupuesto y, como resultado, debemos resaltar que la seguridad en red ocupaba el primer puesto y las soluciones de VPN (redes virtuales privadas) el segundo.

## FACTOR ESENCIAL

En las empresas de hoy en día, especialmente en esta era de actividad reguladora, preservar la integridad, confidencialidad y longevidad de la información empresarial es un factor esencial para lograr el éxito. A medida que nos dirigimos a una economía global basada en la información, el valor y tratamiento adecuado de la misma son cada vez más importantes. El objetivo de cualquier infraestructura de TI es crear sistemas que puedan detectar y protegerse contra los accesos no autorizados sin que ello comprometa la entrada a los usuarios legítimos. La simple denegación del acceso frente a un ataque ya no es aceptable y las redes actuales deben ser capaces de responder a los ataques con el fin de mantener su disponibilidad y fiabilidad al tiempo que se garantiza la continuidad del negocio. La meta de la seguridad debe ser crear redes más robustas haciéndolas también más flexibles.

La mayoría de las empresas españolas apoyan su negocio en las comunicaciones avanzadas proporcionadas por la red que además permite una mejora en la productividad motivos ambos por los que es fundamental asegurar su privacidad. Actualmente, la extensión de las aplicaciones de red a sus oficinas, teletrabajadores, e incluso a terceras partes, es una práctica habitual por lo que los administradores de TI se enfrentan al reto de proteger todos estos entornos y ubicaciones. Uno de los mayores desafíos actuales consiste en ofrecer una

protección eficaz contra los diferentes tipos de ataques posibles sin que esto impacte en la operativa diaria de la empresa.

## MEDIDAS MÁS COMUNES

Las medidas de seguridad más comunes en las redes españolas son la activación de filtros en los routers, la instalación de cortafuegos y la activación de soluciones de VPNs tanto en conexiones entre redes como en comunicaciones remotas. No obstante, estas medidas representan una mínima parte de las posibles soluciones y no atajan la mayoría de los ataques que intentan vulnerar las partes más desprotegidas de la red. Ante este panorama Cisco aporta una solución de seguridad completa con dispositivos de detección y prevención de intrusos, securización de puestos de trabajo y servidores, control de admisión (NAC – Network Admisión Control), seguridad en transmisión de voz, detección y contención de ataques de tipo denegación de servicio, seguridad en entornos WiFi, gestión de identidades en red, sistemas de monitorización y análisis, etc.

La estrategia general de Cisco denominada Red de Información Inteligente o IIN (Intelligent Information Networks) engloba la estrategia de seguridad de Red Auto-Defensiva (Self-Defending Network), cuyo objetivo principal es el de dotar a la red de una capacidad única para identificar, prevenir y adaptarse a las amenazas de seguridad actuales y futuras. De este modo, la red que incorpore los elementos definidos en la solución global de seguridad de Cisco será capaz de auto-defenderse ante posibles ataques.

En definitiva, las empresas se enfrentan a una gran variedad de riesgos para la seguridad de su red, que pueden provenir tanto de elementos externos o internos. Por ello deben saber cuáles son sus puntos vulnerables y cómo minimizar los riesgos. La única defensa eficaz frente a los ataques actuales, dada su complejidad y rapidez de expansión, es mitigar estos riesgos en la propia red.



# El cambiante paisaje de la seguridad

Nos guste o no, las tecnologías de seguridad han cambiado más en los últimos tres años que en los diez anteriores. La extensión de estos cambios, así como su dirección, ha complicado las tareas de los departamentos de seguridad de TI. Antes de considerar el control, vamos a tratar la evolución de este paisaje cambiante.

## EL PERÍMETRO DE SEGURIDAD DE RED

Se trata de uno de los puntos en los que se ha producido mayores cambios, debido al modo en que el

sector enfocaba la seguridad de las redes y la forma en que lo hace ahora tras el cambio en la naturaleza de las propias redes. Y es que en estos momentos una red no puede protegerse simplemente asegurando su perímetro de red; a medida que las empresas han ido consolidando sus centros de datos, creando redes convergentes y adoptando Internet, lo que una vez fue un entorno controlado y auto-contenido está ahora abierto a los socios y colaboradores a través de las extranets entre corporaciones, las conexiones con los puntos de

venta y los empleados que trabajan en casa, por citar algunos ejemplos. Al ampliar la red de la empresa, crecen los límites de confianza para con las redes intermedias y entornos no controlados. Con frecuencia, los dispositivos que se conectan a la red empresarial a través de estas rutas de acceso no son compatibles con las directivas de la empresa. Además, los usuarios utilizan sus dispositivos para acceder a otras redes que pueden no estar controladas antes de conectarse a la red empresarial. Como resultado de esta acción, los dispositivos pueden convertirse en canales por los que penetran ataques o se producen errores por el uso inadecuado.

### TECNOLOGÍA INALÁMBRICA Y MOVILIDAD

En la actualidad, los equipos portátiles, los PDA o Personal Digital Assistant y los teléfonos móviles cuentan con más de una conexión de red. Todos ellos son capaces de establecer redes inalámbricas ad-hoc para habilitar la comunicación con otros dispositivos similares. Además, al nivel de la aplicación, los paquetes de información se pueden enviar eficazmente entre los dispositivos. Como resultado, es mucho más ambiguo conocer dónde empiezan o terminan los límites de una red. Como consecuencia, las empresas tienen que ser capaces de ampliar su control sobre estos dispositivos móviles a fin de administrar el sistema de forma segura y mantener la disponibilidad de la red.

### COMERCIO ELECTRÓNICO Y EXTRANETS

La aparición de interfaces comunes de aplicaciones basados en protocolos de mensajería, como Extensible Markup Language (XML) y Simple Object Access Protocol (SOAP), ha significado un catalizador para el comercio electrónico y la productividad empresarial. Sin embargo, como pasa con la mayoría de las nuevas tecnologías, estos protocolos de mensajería han traído consigo un nuevo conjunto de vulnerabilidades y vectores de ataque a los que las empresas deben enfrentarse. Los datos que antes se difundían a través de varios protocolos de red y podían filtrarse con facilidad a través de directivas de firewall, están ahora combinados dentro de uno o varios protocolos de transporte como, por ejemplo, HTTP en el puerto 80 de TCP. Como resultado, gran parte de los datos que solían residir en las cabeceras de los paquetes se encuentran ahora en su contenido o "payload". Esto crea importantes problemas de procesamiento que permiten a un atacante sortear con relativa facilidad las defensas clásicas de la red. Además, a fin de cumplir con los requisitos de confidencialidad e integridad de los datos empresariales, cada vez más tráfico de este nivel de aplicación se cifra a través de los protocolos SSL/TLS (Secure Socket Layer/Transport Layer Security) y HTTP Secure Socket (HTTPS). Un efecto colateral de esta tendencia es que resulta mucho más difícil para los departamentos TI forzar el cumplimiento de las directivas empresariales de acceso en la red, debido a que no pueden inspeccionar el contenido de los paquetes de estos flujos cifrados.

### VIRUS Y GUSANOS

El número y la variedad de virus y gusanos que han aparecido en los últimos tres años es asombroso. Pero hay dos factores que tienen un enorme impacto en las empresas y su eficacia operativa: el lapso cada vez menor entre el momento en que se detecta la vulnerabilidad y aquel otro en el que se produce el ataque y se expande por toda la empresa. Este hecho ha producido niveles inaceptables de interrupción en el trabajo, además de la necesidad de caros proyectos de recuperación que consumen tiempo, personal y fondos que no estaban originalmente presupuestados para esas tareas.

### NORMAS DE REGULACIÓN

El comportamiento con consecuencias maliciosas que se genera de forma interna en las empresas ha exigido que los organismos de regulación de muchos sectores dicten reglas para la administración del riesgo de la información empresarial. En España existen dos leyes fundamentales en el entorno de la seguridad: la LOPD o Ley Orgánica de Protección de Datos de carácter personal, que tiene por objeto proteger y garantizar las libertades y los derechos fundamentales de las personas físicas, su honor e intimidad personal y familiar; y la LSSI o Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, que regula las actividades de las personas que realizan actividades económicas por Internet u otros medios telemáticos (correo electrónico, televisión digital interactiva...).

Aunque muchas organizaciones asumen de forma errónea que si cumplen con las regulaciones su infraestructura será más segura, no siempre es así. La ley de las consecuencias involuntarias hace que el propio hecho de crear una norma pueda introducir nuevas vulnerabilidades. Por ejemplo, los gusanos y virus pueden expandirse con mayor eficacia en una red que admita las VPNs de extremo a extremo, dado que los nodos intermedios no tienen visibilidad del tráfico transversal. Este tráfico puede llevar gusanos a los servidores empresariales en un paquete cifrado y seguro. Además de que realizar un diagnóstico del ataque lleva más tiempo, dichas VPNs pueden dificultar la resolución del problema.

Llegados a este punto queremos preguntarnos: ¿Puede realmente una red defenderse a sí misma? La respuesta es "Sí". La seguridad de red ha evolucionado desde productos desplegados de forma independiente (como los firewalls) al concepto de sistema global de seguridad. Y Cisco Systems® está en la vanguardia del desarrollo tecnológico que ha hecho que la autodefensa de las redes sea una realidad.

Esta guía que tiene en sus manos describe las razones de Cisco Self-Defending Network, sus fundamentos y los métodos que Cisco Systems ha adoptado para ofrecer este conjunto de capacidades.



# 8 razones para elegir Cisco

Cisco Systems es la compañía con la oferta más completa del mercado de seguridad en red. Éstas son las razones para decidirse por su propuesta.

## 1 Inteligencia segura en la red

En su apuesta por optimizar el despliegue de aplicaciones y servicios sobre la infraestructura de red, Cisco Systems propone una contundente filosofía denominada Red de Información Inteligente o Intelligent Information Network (IIN). Con ella, la multinacional suma mayor inteligencia a la red, al tiempo que logra la optimización de la interacción entre los dispositivos y aplicaciones conectados a la misma. Esta claridad de pensamiento también está articulada en la proposición Self Defending Network, la estrategia de seguridad incluida en IIN con la que el fabricante añade la protección necesaria a la red inteligente.

## 2 Protección presente y futura

El modo en que Cisco Systems articula su propuesta de dotar de mayor inteligencia a la red es un criterio claramente diferenciador con respecto a otras compañías. Y es que, esta proposición permite abordar las necesidades actuales a nivel de seguridad y posibilitar la protección ante ataques de toda índole presentes y futuros. Asimismo, la ingeniería tecnológica de Cisco es capaz de garantizar que las soluciones adquiridas por el cliente en el pasado entren a formar parte de la nueva infraestructura de red que el fabricante propone.

## 3 Soluciones completas de un único proveedor

Cisco Systems es capaz de responder del suministro de toda la infraestructura de red y de la seguridad de la misma. Además, al estar todas las soluciones desarrolladas por el mismo fabricante y disponer de similares interfaces de comunicación y configuración, las labores de implementación, gestión, etc. son más sencillas. En un entorno como la seguridad donde las labores son ya de por sí bastantes complejas, los clientes agradecen enormemente estas facilidades –que se han convertido en uno de los requerimientos clave de todo tipo de usuarios–. Además, esta apuesta por la sencillez también redundará en una importante disminución de los costes, tal y como queda reflejado en el siguiente punto.

## 4 Ahorro en inversión, operación y gestión de la seguridad

Al recurrir a Cisco Systems como único proveedor, una compañía sólo necesitará instruir a su responsable de red en la tecnología de este fabricante, lo que evita tener que invertir ingentes recursos en la formación de profesionales. Además, trabajar con la propuesta de Cisco significa aprovecharse de la activación de todas las funcionalidades de las soluciones de este fabricante. Por ejemplo, la que se refiere a la característica que la compañía ha incorporado en sus conmutadores, Identity Based Networking, con la que consigue que estos dispositivos se relacionen con un servidor de autenticación para participar de las tareas de control de acceso a la red. Así, los switches de Cisco aprovechan las benevolencias de 802.11x al tiempo que aportan funcionalidades extra como la autenticación del usuario en el acceso a redes virtuales o VLANs.

Otro importante ahorro de costes se consigue al ser capaz de optimizar las capacidades de protección de la propia red; y, por consiguiente, minimizar los riesgos de sufrir ataques y tener que afrontar costosos planes de recuperación ante desastres. En este sentido, se evita que la actividad corporativa se vea afectada, asegurando el funcionamiento de la compañía y evitando que la misma tenga que enfrentarse a un periodo de inactividad. Según un informe de Sage elaborado en 2003 y facilitado por Cisco, aquellos clientes que se decidieron por un único fabricante para desplegar una red segura redujeron en un 29% los gastos totales de su infraestructura. En comunicaciones IP, el estudio arrojaba un ahorro del orden del 47%.

## 5 Capacidad de colaboración con terceros

Cisco Systems es consciente de los beneficios que, para su tecnología y sus clientes, pueden derivarse de las relaciones con otros fabricantes. La naturaleza de los ataques es tan variada que un solo fabricante no puede disponer de soluciones de seguridad que solventen todas las situaciones de ataques. Por ello, la colaboración con terceras compañías se convierte en un aspecto clave para proporcionar una solución de seguridad global. En su propuesta NAC (Network Admission Control), Cisco colabora con más de 60 empresas del sector, tales como Computer Associates, F-Secure, IBM, McAfee, Trend Micro, Symantec, Infoexpress, Senforce, WholeSecurity, Panda, etc.

## 6 Compromiso con los comités de estandarización

Los ingenieros de Cisco de Systems participan en los grupos de trabajo de los principales comités de estandarización para aportar su experiencia en la definición de nuevos protocolos y estándares. Con este movimiento el fabricante consigue que sus dispositivos se adhieran al estándar con mayor rapidez y que éste aporte finalmente valor puesto que en su definición se tienen en cuenta los requerimientos del mercado. No obstante, en ocasiones Cisco tiene que desarrollar su propuesta sobre una solución propietaria, mientras espera a su estandarización.

## 7 Productos certificados

Cisco Systems presta especial atención a que sus soluciones de seguridad cumplan con las certificaciones internacionales demandadas en países donde comercializa su porfolio de productos. La certificación de los productos garantiza al cliente que lo publicado por el fabricante en la documentación y descripción de funcionalidades de producto está realmente disponible ya que así se ha comprobado en el proceso de certificación. Cisco es actualmente el único proveedor de conmutadores y routers que dispone de certificación de criterio común EAL-4 para la cualificación de su solución Ipsec en sus routers. La lista de certificaciones por producto Cisco puede consultarse en:

[http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/networking\\_solutions\\_audience\\_business\\_benefit0900aecd8009a16f.html](http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/networking_solutions_audience_business_benefit0900aecd8009a16f.html)

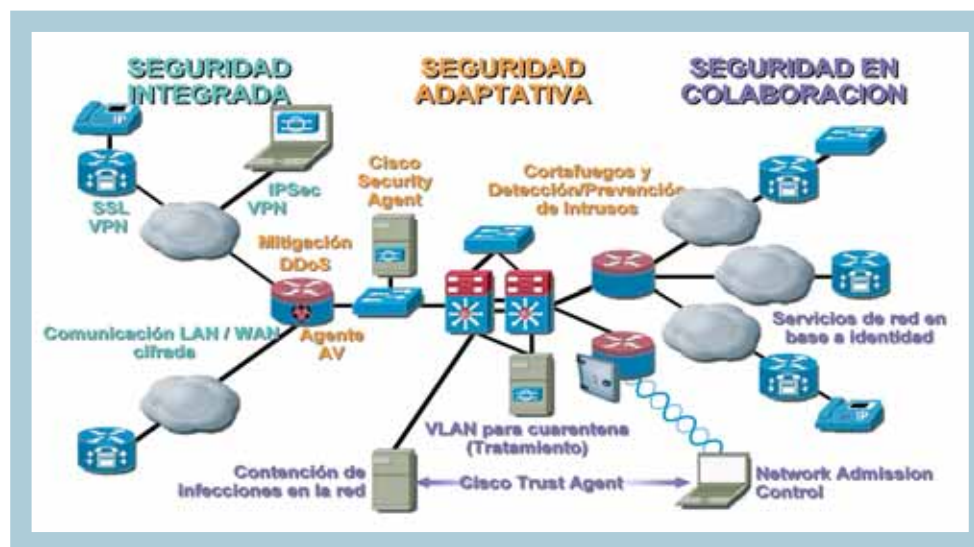
## 8 Compañía por y para el canal

Uno de los aspectos en los que Cisco Systems consigue aportar mayor valor añadido a su propuesta es en el entorno de la formación e incentivos a su red de distribución. Con respecto al primer aspecto la multinacional diseña cursos específicos para acercar a su canal todas las particularidades de sus soluciones. En cuanto a los incentivos, la compañía cuenta con un programa que premia con un porcentaje de margen adicional las ventas realizadas en tecnologías como seguridad y voz.

Asimismo, la firma destaca el importante margen con que opera el canal al trabajar con su catálogo.

# LAS CLAVES DE SELF DEFENDING NETWORK

Bajo el paraguas de Intelligent Information Network (IIN o Red de Información Inteligente), Cisco Systems define su particular visión de sumar a la red mayores niveles de inteligencia para optimizar la integración de aplicaciones y servicios sobre la misma. Para su implantación, IIN necesita una solución de seguridad capaz de garantizar el funcionamiento optimizado del sistema completo; y eso es lo que aporta Self Defending Network (SDN o Red Auto-Defensiva). Con esta estrategia de seguridad, el fabricante adereza este movimiento de inteligencia en la red y abre las puertas a un futuro donde las infraestructuras asumen su propia protección. Self Defending Network posibilita la introducción de funcionalidades de protección en todos los dispositivos de la red, facilita la conexión a aquellos dispositivos (portátiles, PDAs, etc.) que dispongan de antivirus y parches actualizados, y permite que la red se autodefienda y se adapte a ataques presentes y futuros.



## TRÍADA DE FASES

Self Defending Network está articulada en torno a tres fases, en las que, según se va escalando, se alcanza un nivel más completo de protección. La primera fase (Fase I, o de Seguridad Integrada) se refiere a la integración de las funcionali-

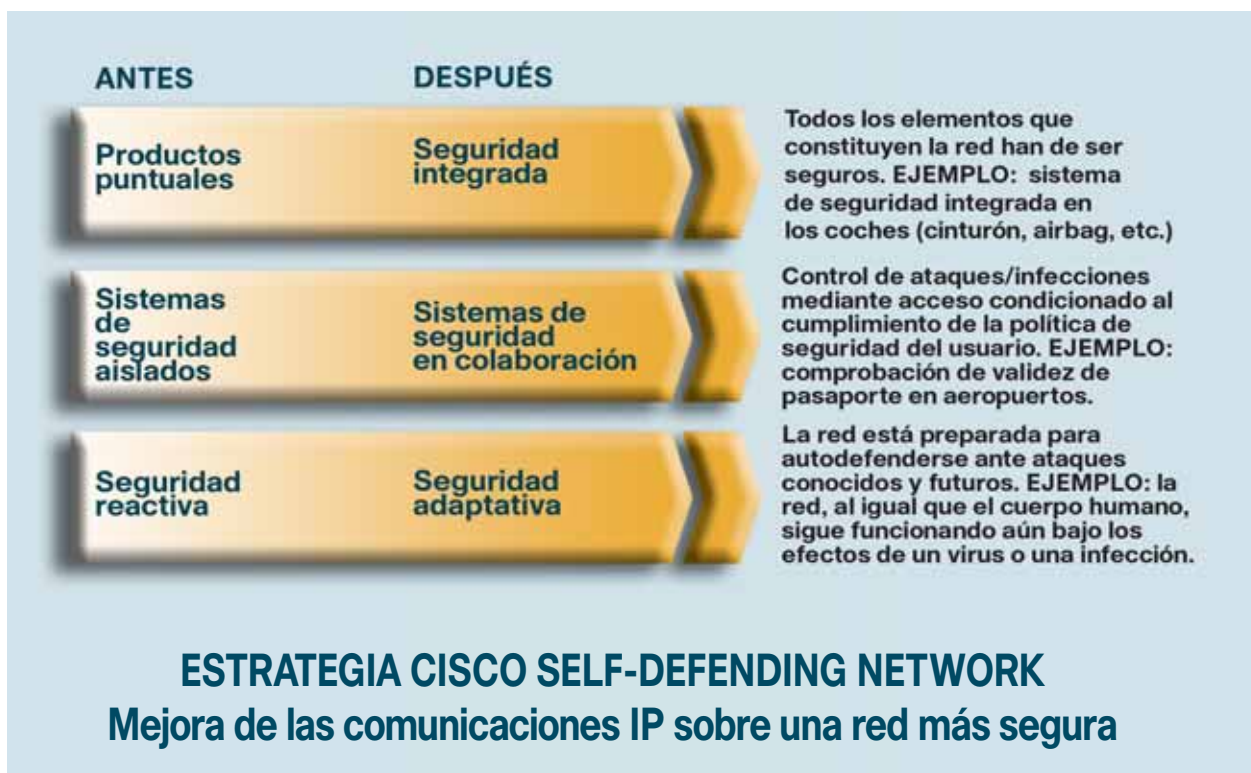
dades de seguridad en todos los productos que desarrolla la compañía, lo que no implica que puedan comunicarse con otros dispositivos de la red. La solución a esta cuestión llega una vez se alcanza la segunda fase (Fase II o de Seguridad Colaborativa), bautizada así porque

supone el pistoletazo de salida a la propuesta de infraestructura NAC (Network Admission Control, o Arquitectura de Control de Admisión en la Red) del fabricante, por la cual se facilitan las primeras implementaciones de cómo los sistemas de seguridad pueden interactuar entre sí. Los primeros en llegar a esta etapa de colaboración fueron los routers y concentradores VPN de la compañía, mientras que los switches y soluciones WiFi acaban de arribar, tras el reciente lanzamiento de NAC II. Gracias a NAC los routers, concentradores VPN, conmutadores y dispositivos WiFi, participan en el proceso de admisión o denegación de un dispositivo desde el que el usuario quiere acceder a la red. Para ello, los dispositivos de red se comunican con los servidores de autenticación, que opcionalmente pueden consultar a servidores de gestión de políticas de seguridad, al servidor de antivirus o al servidor de auditoría para comprobar la identidad y el nivel de protección del dispositivo. Como vemos, en este estadio, las soluciones de red mencionadas presumen

de capacidades integradas de seguridad, y además, ahora, de colaboración.

Por último, la tercera fase (Fase III o de Seguridad Adaptativa) da un paso más y con ella evoluciona el concepto de colaboración para conseguir un entorno donde la propuesta de seguridad se culmina con avanzadas facultades de automatización y de autodefensa. Se llama “Adaptativa” porque los dispositivos (los cortafuegos, por ejemplo) cuentan con la suficiente inteligencia como para “adaptarse” a una situación de ataque mediante el control y mitigación de los efectos del mismo. Las facultades de automatización quedan así definidas, mientras que las de autodefensa se refieren a la capacidad de responder activamente ante las amenazas. En este escenario, la red es capaz de reaccionar cada vez con mayor rapidez ante ataques que con el tiempo se han perfeccionado y son más veloces.

Esta tercera fase de la estrategia Self Defending Network de Cisco acogerá las próximas soluciones de seguridad que la compañía introduzca en el mercado.



# FASE I

# SEGURIDAD INTEGRADA

Como veíamos en las páginas anteriores, la primera de estas tres fases en las que Cisco Systems articula su propuesta Self Defending Network (SDN, o Red Auto-Defensiva) es la denominada **Fase I o de Seguridad Integrada**, que se refiere a la integración de las funcionalidades de seguridad en todos los productos que desarrolla la compañía.

Obviamente, la introducción de unas u otras características de seguridad en cada una de estas soluciones dependerá de la función de las mismas en la infraestructura de red. Así, un router podrá beneficiarse de capacidades de filtros de protección, cortafuegos, VPN, etc.; mientras que éstas serían innecesarias para un punto de acceso Wi-Fi, que sólo requiere de capacidades de seguridad aplicables a una red wireles.

## SOLUCIONES INCLUIDAS

En esta primera fase, el objetivo es integrar la seguridad en cualquier producto o desarrollo sobre el que trabaje Cisco; es decir, en todas y cada una de las soluciones de seguridad que diseñan y desarrollan sus más de 1.500 ingenieros dedicados en exclusiva al área de seguridad. En ella se consiguen, a nivel de aplicaciones, el acceso seguro mediante SSL (Secure Socket Layer), y se extienden las benevolencias de IPsec a los routers creados en el seno de la compañía.

De esta manera, en la primera fase se realiza la integración en los productos de las funcionalidades de seguridad IPsec VPN, SSL VPN, y concentradores VPN. Las soluciones VPN de Cisco son aplicables tanto a la conexión entre redes como a la conexión remota de usuarios. También se incor-

para comunicación LAN/WAN cifrada, y características de cortafuegos en routers y conmutadores.

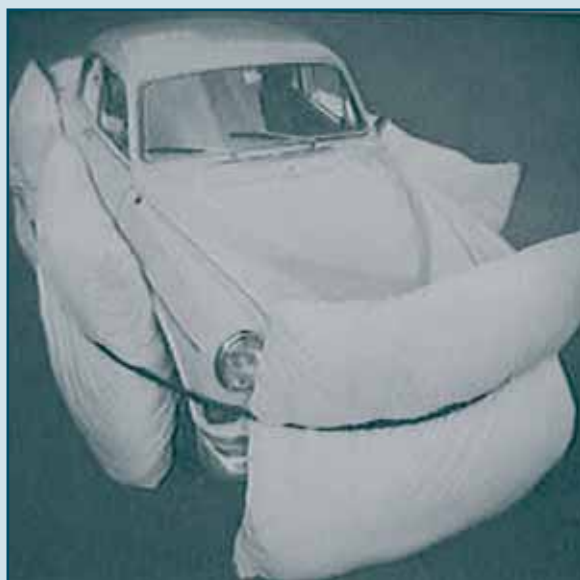
Este deseo de incrementar la protección en el perímetro de las redes está relacionado con la transformación natural que han experimentado las infraestructuras a lo largo de los últimos tiempos. El cambio en el planteamiento de cómo dotar de seguridad a las redes ha sobrevenido una vez que las corporaciones han tenido consolidados sus centros de datos, han hecho converger sus redes internas y han abrazado Internet. En la actualidad a una red empresarial pueden tener acceso clientes y proveedores gracias a la proliferación de extranets, entre otros motivos.

Dada esta situación, una red necesita disponer de dispositivos internos con un nivel de seguridad integrada cada vez más notable. Y cuatro son los apartados donde esa integración cobra mayor significado. El primero de ellos es el relativo a la identidad, en virtud del cual se consiguen soluciones optimizadas en la

periferia. Las soluciones estándar de gestión de identidades de usuarios en red basado en puerto de acceso (802.1x) están soportadas por los conmutadores Cisco que opcionalmente permiten la activación de una versión mejorada de la gestión de identidades en red desarrollada por Cisco que se denomina Identity-Based Networking Services (IBNS). IBNS realiza la autenticación del usuario en base al puerto de acceso y además permite la asignación dinámica de VLANs y filtros por usuario.

El segundo de los apartados en los que se produce la integración de seguridad se centra en la protección de la infraestructura de red, mediante la definición de filtros, mecanismos de control del consumo de ancho de banda, monitorización detallada con la activación de Netflow, etc.

El tercero es el referido a la conectividad segura a través de la incorporación del cifrado de los datos; y el cuarto, y último, se ocupa del acceso seguro a las aplicaciones mediante la solución de SSL VPN que en Cisco se denomina Web VPN.



### SEGURIDAD A POSTERIORI

Hace años los coches no incluían suficientes elementos de seguridad para proteger la vida del conductor y los pasajeros. Es decir, la seguridad no estaba integrada en su diseño inicial. A día de hoy, eso es lo que ocurre con algunas compañías que no integran la seguridad en sus soluciones, sino que van resolviendo este problema a base de parches.



### SEGURIDAD INTEGRADA

Al igual que en la actualidad un automóvil incluye en su diseño inicial toda una serie de elementos de protección creados para aumentar la seguridad del conductor y de los pasajeros; la arquitectura de Cisco Systems, Self Defending Network, contempla, ya en su primera fase, la incorporación de funcionalidades de seguridad para todos los productos que desarrolla la compañía.

# FASE II

# SEGURIDAD COLABORATIVA

El segundo estrato de Self Defending Network es el que ha quedado bajo el rótulo de **Fase II o Seguridad Colaborativa**. Y es en este espacio bajo el cual se engloba la propuesta de infraestructura NAC (Network Admission Control, o Arquitectura de Control de Admisión en la Red) del fabricante, donde se realizan las primeras implementaciones para que los sistemas de seguridad pueden interactuar entre sí.

Como manera de consolidar esta entrega NAC o de colaboración, Cisco Systems ha dado vida al programa del mismo nombre, con el que comparte apuesta tecnológica con los más de 60 fabricantes que participan en la iniciativa. Bajo ella, los integrantes diseñan y comercializan aplicaciones cliente/servidor, así como propuestas de servicios que incorporan funcionalidades compatibles con la infraestructura NAC. Si desea más información sobre los partners NAC visite:

<http://www.cisco.com/en/US/partners/pr46/nac/partners.html>

## APORTACIONES

La segunda fase de la propuesta Self Defending Network permite controlar el

acceso a la red de los distintos dispositivos, imposibilitando la entrada de aquellos que no cumplen con los requisitos mínimos de protección exigidos por la política de seguridad previamente definida por la compañía.

En este sentido, los componentes que integran la red pueden realizar una labor conjunta de protección de la infraestructura, permitiendo o restringiendo el acceso de los usuarios en función de su identidad y del nivel de protección de su máquina: estado de actualización del sistema operativo (Service Packs en Windows), versión y estado de actualización del antivirus, presencia de software cliente de seguridad, etc.

En este entorno es donde se despliega toda la potencia de la solución NAC, en la que interactúan los dispositivos de red: routers, concentradores de VPN, conmutadores y dispositivos WiFi con los servidores de gestión de política de seguridad. En el instante en el que los dispositivos de red detectan el intento de acceso desde un dispositivo cliente a la red, contactan con el servidor de autenticación que, a su vez, y de forma opcional, puede contactar con



En su segunda fase Cisco controla el acceso a la red de los distintos dispositivos, imposibilitando la entrada de aquellos que no cumplen con los requisitos mínimos de protección exigidos por la política de seguridad previamente definida por la compañía. En la vida real lo podríamos comparar con lo que ocurre en los aeropuertos con la comprobación de la validez del pasaporte.

## APPLIANCE NAC

Gracias a la solución de NAC appliance o Cisco Clean Access, se permite la activación del control de admisión en redes cuyos dispositivos de red no incorporen aún la solución de NAC o sean de otras marcas.

Ofrecida en modo appliance, esta alternativa propone una respuesta similar a la descrita anteriormente pero es aplicable a redes heterogéneas y de menor tamaño.

Los componentes de la solución NAC appliance (Clean Access Server, Clean Access

Manager, cliente Clean Access y servicios de suscripción) permiten un despliegue sencillo y rápido de la solución de control de acceso en redes pequeñas o en partes de la red que requieran una actuación inmediata ya que son más vulnerables ante posibles infecciones propagadas por los dispositivos que normalmente se conectan a ellas (por ejemplo, segmentos de red dedicados a dar conectividad a dispositivos de terceras compañías en su tránsito por la red corporativa).

el servidor de antivirus, el servidor de gestión en políticas de seguridad y el servidor de auditoría. Así comprueban que el posible nuevo inquilino cumple con la política de seguridad definida. Recordemos que Cisco dispone de un servidor de autenticación propio denominado Cisco Security Access que soporta tanto RADIUS como TACACS y es el utilizado dentro de la solución NAC como servidor de autenticación. Asimismo, Cisco distribuye de forma gratuita el software cliente denominado Cisco Trust Agent que se instala en los ordenadores en los que se quiere activar el control de admisión.

Dentro de la fase 2 de NAC recientemente incorporada a la solución, existe también la opción de activación del control de acceso a ordenadores que no disponen del software cliente Cisco Trust Agent. Esto se consigue mediante la colaboración del servidor de autenticación con soluciones de auditoría que se basan típicamente en la utilización de escáneres que comprueban el estado del ordenador antes de emitir un informe sobre su estado de salud.

Además, en la fase 2 se incrementa el control de las condiciones de acceso a la red al mejorar la capacidad de ésta de res-

ponder ante ataques. No sólo eso, sino que, gracias a los acuerdos que Cisco mantiene con sus socios colaboradores en NAC, esta alternativa cuenta igualmente con remozadas funcionalidades de automatización de las distintas funciones de seguridad. Por ejemplo, más allá de controlar si el dispositivo cuenta con los parches antivirus necesarios para acceder a la infraestructura, se puede, gracias a la tecnología de Tivoli, automatizar la descarga de las actualizaciones. De este modo, el usuario no tendrá que saber dónde se encuentra el parche, para después proceder a una descarga manual, puesto que la red asumirá todo el proceso.

# FASE III

# SEGURIDAD ADAPTATIVA

La **Fase III o de Seguridad Adaptativa** hace evolucionar el concepto de colaboración para conseguir un entorno donde la propuesta de seguridad culmina con avanzadas facultades de proactividad, automatización y de autodefensa.

Una de las soluciones pertenecientes a esta fase que mejor ilustra la adaptabilidad de la solución ante ataques es la de mitigación de ataques DDos (Dinamic Denial of Service) que permite la detección, control y mitigación de los efectos de ataques de denegación de servicio en modo dinámico. La solución utiliza dos componentes basados en módulos instalables en los conmutadores Catalyst 6500: módulo Traffic Anomaly Detector y módulo Guard. El primero funciona a modo de sonda ya que monitoriza el tráfico de red para crear patrones de tráficos

típicos en la red y es a partir de esta información como logra detectar aumentos de tráfico anómalos en la red que normalmente proceden de atacantes cuyo objetivo es dejar fuera de servicio un servidor destino. Una vez detectado el posible ataque de denegación de servicio, el tráfico es redirigido al módulo Guard que analiza y limpia todo el tráfico. El módulo Guard descarta el tráfico malicioso para dejar pasar el tráfico legítimo hacia el servidor destino de forma que la solución ataja completamente el ataque, ya que sin necesidad de desactivar el servidor de destino se evita que dicho servidor procese el tráfico proveniente de la fuente atacante.

## EN LA RETAGUARDIA

En esta última entrega, donde se consigue el nivel más elevado de seguridad, se logra que la red, defi-



En su tercera fase Cisco logra que la red asuma su propia defensa. De todos modos, la red, al igual que el cuerpo humano, sigue funcionando aún bajo los efectos de un virus o una infección.

nitivamente, asuma su propia defensa. Y lo hace apoyándose en soluciones del tipo IDS, IPS, cortafuegos... –tanto en versión appliance, como en su modalidad de placa instalable en el conmutador modular Catalyst 6500–, y en soluciones de mitigación de ataques de denegación de servicio (DoS), etc.

En este estrato hemos de mencionar las siguientes soluciones: la propuesta de mitigación de ataques de denegación de servicio mediante la combinación de los módulos Cisco Traffic Anomaly Detector y Cisco Guard; la solución Cisco Security Agent (CSA), que, instalada tanto en servidores como en estaciones de trabajo detecta intentos de modificación del sistema operativo (por ejemplo, intento de modificación de registros en Win-

dows) o la modificación de parámetros del sistema y lanza un mensaje de alarma para que el usuario evite la instalación del tráfico malicioso; la propuesta ASA (Adaptive Security Appliance), que integra en una sola caja las funciones de cortafuegos, terminación de VPN, e IDS-IPS; y las soluciones antiX (antivirus, antispam, etc.), donde destacan los IDS/IPS y la propuesta de Cisco Secure Desktop. Tampoco podemos olvidar las aplicaciones de gestión de Cisco que permiten una gestión gráfica y sencilla de sus diversas soluciones de seguridad: Security Device Managers, Cisco Works VMS, Cisco Secure MARS o CS-MARS (Security Monitoring, Analysis and Response System), y Security Auditor son algunas de las aplicaciones disponibles en el porfolio de aplicaciones de gestión de Cisco.



# Acceso seguro a través de routers y conmutadores

**Network Foundation Protection** es la apuesta de Cisco para proteger la infraestructura de red de ataques directos, así como de fallos en configuraciones, o actos involuntarios que pueden poner en riesgo la infraestructura de red. El objetivo de estas funcionalidades es proporcionar el funcionamiento o acceso a los dispositivos durante períodos de ataques en la red. Así pues, existen funcionalidades como **AutoSecure**, que permite minimizar el impacto en errores de configuración, así como desactivar servicios no utilizados que son potencialmente utilizables para ataques. **Control Plane Policing** es el nombre de otra funcionalidad muy interesante que permite actuar sobre diferentes elementos de la infraestructura para preservar el acceso a los dispositivos de red durante períodos de ataques. Otras funcionalidades, tales como **control de uso de CPU y memoria, gestión de los datos mediante mecanismos de calidad de servicio, control de acceso a la red**, etc., permiten dotar al centro de datos de una infraestructura de seguridad integrada en todos los dispositivos de red.

Existen otras tecnologías tales como Cisco Express Forwarding (CEF), Quality of Service (QoS), Private VLAN, Netflow (Gestión del tráfico de red), CAR (Committed Access Rate), etc., que colaboran muy estrechamente en preservar la infraestructura de red de los potenciales ataques a que puede ser sometida y que están disponibles en la familia de conmutadores de Cisco. Adicionalmente, Cisco IOS Security es un conjunto de funcionalidades implementadas en plataformas de routers mediante el cual se puede securizar la red. Entre ellas está el IOS Firewall, que es una implementación software de cortafuegos en un router.

## ROUTERS DE SERVICIOS INTEGRADOS

En septiembre del año pasado, Cisco presentó su revolucionaria apuesta por los

routers de servicios integrados (ISR, o Integrated Services Routers), compuesta en aquel momento por los modelos 1800, 2800 y 3800 y que, posteriormente, en mayo de 2005, se completó con el anuncio de la familia ISR 800. Se trata de la primera propuesta de toda la industria con virtualización incluida que además incorporaba funcionalidades de voz y seguridad, facilitando el despliegue y desarrollo de los servicios de convergencia a una velocidad continua de banda ancha. Los ISR de Cisco permiten la activación de forma opcional de servicios de cortafuegos, VPN e IPS dentro de la propia plataforma.

## GESTIÓN DE IDENTIDADES EN RED

Con las soluciones de gestión de identidades y relaciones de confianza de Cisco, esencialmente se proporciona autorización y control de acceso a la red, se obliga al cumplimiento de políticas definidas para el acceso a todos los recursos y se determinan los privilegios de acceso a la red basados en las políticas de acceso definidas. Esta tecnología comprende a su vez: gestión de identidades (AAA), servicios de red basados en Identidades (IBNS: Identity Based Networking Services) que es una extensión mejorada de la solución 802.1x, y Control de Admisión a la Red (NAC: Network Admission Control). Los beneficios de la gestión de acceso a la red son, entre otros, los siguientes: flexibilidad y movilidad de usuarios y dispositivos de acceso; conectividad segura a todos los recursos de la red; gestión centralizada de acceso y reducción de costes de implementación.

## TAMBIÉN OFRECEN SEGURIDAD...

● **VPNs punto a punto:** ofrece conectividad segura para extender la red corporativa a oficinas remotas, teletrabajadores e intranets y extranets con Cisco rou-

ters, Cisco PIX Security, o Cisco Catalyst 6500 Security Services Modules.

● **VPNs de acceso remoto:** permite a los usuarios conectarse desde internet a la red corporativa independientemente del sitio en el que se encuentre, a cualquier hora, a través de Cisco VPN 3000 Series Concentrators y Cisco VPN Client o Cisco WebVPN. Otros productos Cisco que nos proporcionan esta solución son también Cisco routers, Cisco ASA 5500, PIX Security Appliances, y Catalyst 6500 Series Switches.

● **Gestión y monitorización:** a través de CiscoWorks VPN/Security Management (VMS), y gestores de dispositivos Cisco Security Device Manager (SDM), VPN Device Manager (VDM), y PIX Device Manager (PDM). Todas ellas permiten: controlar los costes e incrementar la flexibilidad, reducir tiempo de despliegue e incrementar el control con políticas centralizadas, reducir el coste de propiedad utilizando la actual base instalada, disminuir los costes en infraestructura de conectividad, e incrementar la productividad. Además, dicha propuesta ofrece una solución robusta para VPN en IPsec y VPN SSL.

La solución en IPsec permite el acceso remoto a los usuarios que requieren de aplicaciones de datos, voz y vídeo de la red de la compañía desde diferentes localizaciones. La solución Cisco EasyVPN proporciona este tipo de conectividad privada mediante un entorno cliente/servidor. Por último, Cisco WebVPN es la solución de acceso remoto desde cualquier dispositivo basado en SSL, con tan sólo un navegador. Dicha herramienta proporciona tres niveles de acceso, sin cliente, con plug-in (mapeo de puertos) o con cliente SSL, dependiendo de las necesidades.

# WLANs protegidas

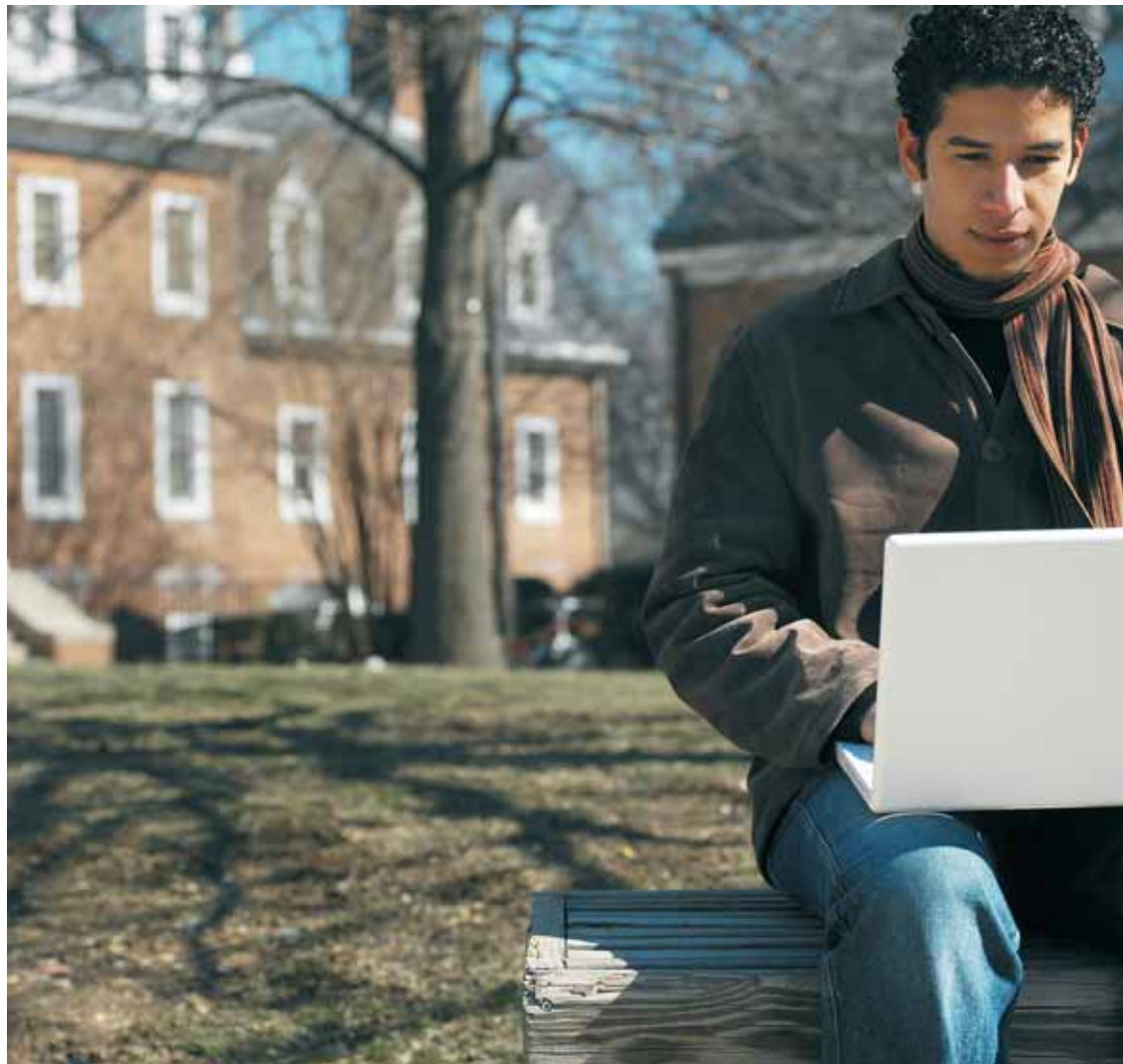
Para nadie es un secreto que una de las trabas iniciales del desarrollo de la tecnología inalámbrica fue la falta de confianza en la seguridad de estas infraestructuras. Sin embargo, a día de hoy esta propuesta cuenta con todas las soluciones necesarias para llegar a ser tan fiable como la opción cableada. La seguridad en entornos WiFi es una combinación de autenticación y cifrado de la comunicación y en estos entornos normalmente se habla de cifrado WEP (Wired Equivalence Privacy) y autenticación EAP (Extended Authentication Protocol). Cisco ofrece una seguridad mejorada a través de la solución Cisco Wireless Security Suite proporcionando soporte completo WPA y WPA2 (Wi-Fi Protected Access). Las características principales de esta solución son la autenticación mutua, la gestión dinámica de claves y el cifrado de los datos a través de AES (Advance Encryption Standard).

El objetivo es conservar la integridad de los datos, proteger la confidencialidad de los usuarios y dispositivos, y asegurar la disponibilidad de la red y de las herramientas. Para mantener una infraestructura protegida se puede recurrir a la seguridad WLAN. En función de ella, primero hay que aplicar los parámetros previstos para el sistema, monitorizar su funcionamiento, intentar mejorar nuestra propia protección y, después, aplicar las mejoras pertinentes a nuestro sistema. En este sentido, la seguridad debe alcanzar a todos los componentes de esta red wireless: tarjeta de red, punto de acceso, puentes y antenas. Los beneficios que nos proporciona esta solución son conectividad segura para redes inalámbricas, gestión de identidades y defensa ante amenazas en redes wireless.

## CISCO WIRELESS SECURITY SUITE

En este escenario, la solución Cisco Wireless Security Suite, para productos de la serie Cisco Aironet y dispositivos cliente Cisco Compatible, se presenta como una solución de seguridad WLAN empresarial basada en estándares, que proporciona a los administradores de red la privacidad y confidencialidad que sus datos necesitan.

Por otro lado, la propuesta Cisco Integrated Wireless Network, integrada en la



filosofía Cisco Self-Defending Network, redundando en la consecución de una opción WLAN escalable, gestionable y segura, con uno de los costes totales de propiedad más bajos. Se trata de una evolución de la alternativa Cisco Structured Wireless Network, disponible en el portfolio del fabricante desde 2003. Además, Cisco Integrated Wireless Network incluye dos soluciones WLAN de clase empresarial: Cisco Distributed WLAN Solution y Cisco Centralized WLAN Solution. También reúne un conjunto de nuevas soluciones, basadas en la tecnología de la firma adquirida recientemente por Cisco, Airspace. Aquí se cuentan los puntos de acceso Cisco Aironet 1000 Series Lightweight, los controladores Wireless LAN de las series 2000, 4100 y 4400, la solución Cis-

co Wireless Control System (WCS) y el appliance Cisco Wireless Location.

## EL VALOR DE LA INTEGRACIÓN

En la actualidad, el incremento de implantaciones de WLAN es notable, tendencia que empieza a tener un alto impacto en las infraestructuras LAN existentes. Así, cada vez se otorga mayor importancia a componentes como firewalls; directorios de usuarios; servidores de autenticación, autorización y administración (AAA), directorios de usuarios, etc. Por todo ello es vital integrar la propuesta wireless con la red cableada de la que se puede aprovechar todo su potencial de seguridad. Lo contrario supondría un pobre uso de los recursos corporativos, debido a la ineficiencia de un escenario empresarial basado en redes paralelas.

# Comunicaciones de voz segura

Una de las suposiciones más comunes en el ámbito de la VoIP tiene que ver con la hipotética insuficiencia de seguridad en estas infraestructuras. Se piensa que una solución “híbrida” de telefonía tradicional y red de datos IP es más segura que otra que emplee la tecnología IP para el total de las comunicaciones corporativas. Pero esta apreciación no es real, ya que las soluciones de comunicación basadas en IP son igual de seguras y fiables o más que las soluciones de transmisión de voz tradicionales.

En este sentido la seguridad de las comunicaciones de voz es también un factor diferenciador de la solución de Cisco, ya que

todas las medidas de seguridad en la infraestructura de datos son aplicables a la transmisión de la voz una vez que ambas redes convergen. Adicionalmente en Cisco se añaden aplicaciones de software de protección del servidor sobre el que se ejecuta el procesamiento de las llamadas (Call Manager), se permite el cifrado de las conversaciones de voz, la autenticación de los terminales telefónicos e incluso la gestión del sistema puede realizarse en modo seguro.

## TRES FOCOS

Para lograr una infraestructura de comunicación IP segura, Cisco tiene en cuenta la securización de la infraestructura de red, la

protección del equipamiento de telefonía IP, y los procesos de autenticación y encriptación de la telefonía IP.

En el primero de estos apartados, se requiere una combinación de tecnologías y actuaciones para salvaguardar la infraestructura para servicios de datos, voz y vídeo. Entre éstas, destaca la separación de la voz y los datos en las redes virtuales o VLANs, la activación de mecanismos de protección en los conmutadores como la configuración de mecanismos de control de QoS, el uso de cortafuegos para las transmisiones de voz, la utilización de sistemas de prevención y detección de intrusiones, la utilización de soluciones de conectividad segura, con tecnologías como IP Security (IPSEC), SSL y VPN, la incorporación de medidas de seguridad a la conectividad sin cable, etc.

En lo que respecta a la protección del equipamiento de telefonía IP –donde se hallan los teléfonos IP y el servidor de procesamiento de llamadas Cisco Call Manager–, han de salvaguardarse el perímetro y los canales de comunicación de la infraestructura. Los pasos que han de tomarse en este sentido incluyen el fortalecimiento de los teléfonos IP mediante autenticación de los dispositivos que intervienen en la comunicación de voz y datos. Los teléfonos IP incluyen una clave que permite la autenticación del dispositivo y, de manera opcional, el cliente podrá crear sus propias claves de identificación. En cuanto a la protección del servidor con Call Manager, que realiza las labores de procesamiento de llamadas, Cisco incluye su solución de detección de intrusos en host o Cisco Security Agent, que en combinación con la solución de detección y prevención de ataques de denegación de servicios protege al servidor de los ataques más típicos en los entornos de voz.


Adicionalmente, Cisco aporta soluciones que combaten el fraude en las comunicaciones de voz, posibilitando el bloqueo de llamadas a líneas externas, internacionales, etc.



poweredbycisco.  
**nomolestar**

Un hotel en Barcelona. Un retraso en Londres. Un café en Madrid.  
 Lugares perfectos para que ideas e inspiración encuentren el camino a su negocio. Entre en la red de Autodefensa de Cisco Systems, con control de admisión de redes. Se adapta a nuevos entornos de amenazas ya que frena los ataques antes de que ocurran. De forma automática, proactiva e intuitiva. Aprenda como las redes de autodefensa aseguran su negocio en [www.cisco.com/poweredby](http://www.cisco.com/poweredby)

CISCO SYSTEMS

seguridad. powered by 

# Productos y servicios para pymes

Para Cisco Systems, el término pyme engloba a corporaciones de hasta 250 puestos de trabajo. Dicho entorno integra, junto con el relativo a mid-market, el negocio que el fabricante ha bautizado como Cisco Comercial. Recordemos que los otros dos ámbitos en los que la firma americana estructura su negocio en nuestro país son Administración Pública y Enterprise (banca, seguros, industria...). El peso de Comercial en la facturación de Cisco España al cierre de su año fiscal 2005, concluido el pasado 31 de julio, ascendió a un 40%, según **Fernando Rojo, director de canal de Cisco Systems España.**

Tras más de dos años de medir sus fuerzas en la pyme, Cisco ha convertido este entorno en uno de sus focos de negocio más estratégicos. Tal y como apunta la propia corporación, las empresas, sea cual sea su tamaño, tienen necesidades básicas similares, aunque las necesidades tecnológicas no son las mismas. Por este motivo, Cisco ha desarrollado un portafolio de soluciones pyme diseñado para dar respuesta a las necesidades de dichas empresas. Esta alternativa ayuda a que las organizaciones obtengan el máximo partido de sus redes, proporcionando mejores capacidades en las áreas de voz, seguridad, movilidad y un mayor retorno de la inversión. ➤

## NECESIDADES DE UNA PEQUEÑA Y MEDIANA EMPRESA

1. Trabajar de modo más eficiente y con un grado de colaboración mayor
2. Ganar en productividad y rentabilidad, ya sea en la oficina, en casa o durante un viaje
3. Contar con una infraestructura que ayude a crear un equipo y unos recursos de trabajo interconectados
4. Disponer de un sistema diseñado para proteger los activos más importantes de la empresa frente a amenazas internas y externas
5. Administrar los requerimientos corporativos de voz, datos y vídeo
6. Herramientas que permitan simplificar la administración
7. Mayor productividad de los empleados
8. Mejor satisfacción del cliente
9. Menores costes operativos



# EASY RENTING

**Easy Renting** es el nombre con el que Cisco Systems ha bautizado su última iniciativa diseñada específicamente para el mercado pyme. El fabricante financia bajo esta modalidad la adquisición de sus soluciones en este ámbito empresarial, facilitando a estas corporaciones la obtención de importantes incentivos fiscales.

**Easy Renting** propone una herramienta muy útil que facilita a los distribuidores la solicitud de créditos, el cálculo de cuotas y la petición de autorizaciones para poder ofrecer al cliente final la solución que mejor se adapte a sus necesidades. Y ello con una financiación individualizada. Pocos días después, una vez concluida la operación y entregados los productos, el partner recibe el total de la cantidad, eliminando la gestión de cobros y mejorando el flujo de caja.

“Una de las ventajas más importantes del programa **Easy Renting** para el cliente de Cisco Systems es que todos los gastos que realice son deducibles, con lo que se reducirán a su vez los impuestos sobre beneficios que tenga que abonar”, asegura Fernando Rojo, director de canal de Cisco Systems España. “Además, al tratarse de pagos flexibles, las empresas pueden adaptarse a su propio flujo de trabajo de liquidez y disfrutar siempre de las últimas novedades tecnológicas”.

Para más información sobre el programa **Easy renting** visite la siguiente dirección web: [www.cisco.es/easyrenting](http://www.cisco.es/easyrenting)

## ➤ SOLUCIONES A MEDIDA

En su esfuerzo de aunar recursos enfocados al entorno pyme, Cisco presentó a mediados de septiembre su propuesta **Cisco Business Communications Solutions**, en la que contempla tres aspectos. En primer lugar, cinco familias de soluciones específicas: routers de servicios integrados; switches Cisco Catalyst Express 500; soluciones inalámbricas Aironet; productos específicos de seguridad –ya sean soluciones que integran una o varias funcionalidades de protección–; y soluciones de telefonía IP, como Call Manager Express. En segundo lugar, el fabricante proporciona servicios de soporte y mantenimiento agrupados bajo **Cisco SMB Support Assistant**. En último término, Cisco ofrece un servicio de financiación que en España se ha materializado en la iniciativa **Easy Renting**.

Como primera propuesta dentro del conjunto de Soluciones para pymes, Cisco Business Communications Solutions, la multinacional nos presenta la Solución de red sólida y segura de Cisco o Secure Network Foundation, capaz de transmitir su mensaje al escenario de las pequeñas y medianas empresas. “Con ella pretendemos explicar a todas las pymes españolas en qué consiste esta solución de negocio específicamente diseñada para ellas. La propuesta es el resultado de una investigación de mercado que realizamos con nuestros clientes actuales y potenciales, gracias a la cual conocimos qué tipo de soluciones estaban demandando y observamos que los aspectos más valorados eran la sencillez de utilización, la seguridad integrada, la fiabilidad y su asequible precio. En este sentido, ideamos un completo porfolio de soluciones para crear una estructura IP segura; y completamos la propuesta con servicios asociados de mantenimiento y soporte; y otros relativos a financiación”, explica **Xavier Massa**, director comercial para pymes de Cisco.

La Solución de Red Sólida y Segura de Cisco permite tener una infraestructura de red sólida, fiable y segura, que ayuda a simplificar las operaciones, reducir costes, protegerse contra las

crecientes amenazas de red y dedicar menos tiempo a los problemas de mantenimiento. Dicha solución ha sido diseñada con protección integrada. Las características de seguridad se han diseñado para detener a los intrusos antes de que causen algún daño, eliminando las interrupciones ocasionadas por gusanos, virus y hackers, de forma que todo pueda funcionar correctamente. Así, las pymes pueden disponer en su red de características avanzadas, gracias a nuevos niveles de sencillez de uso. El nuevo switch Cisco® Catalyst® Express 500 y su interface gráfica de usuario hacen que la instalación y administración sean sólo cuestión de seleccionar una opción y realizar un simple click. Para conocer en detalle las Soluciones Cisco para pymes, Business Communications Solutions, puede visitar la siguiente dirección web:

[www.cisco.es/basesolida](http://www.cisco.es/basesolida).

## PRODUCTOS

Dentro de su propuesta Cisco Business Communications Solutions, la compañía integra, tal y como veíamos, cinco grupos de productos. Con respecto al primero de ellos, los **routers de servicios integrados (ISR, Integrated Services Routers)**, Massa argumenta que “con estos nuevos routers facilitamos el acceso a redes de banda ancha, y lo hacemos de forma segura y eficaz. Además, también logramos incorporar amplias funcionalidades de seguridad en los dispositivos”. Bajo estas dos características que destaca el directivo se presentaron en sociedad los primeros routers de servicios integrados que lanzó la compañía en septiembre del año pasado, los modelos 1800, 2800 y 3800. Con el modelo 800, Cisco incorporó capacidad inalámbrica, y, posteriormente, soporte para telefonía IP.

Concretando las ventajas de esta gran apuesta para las pymes, los routers de servicios integrados de Cisco se presentan como un catalizador que conecta diferentes redes y proporciona el soporte necesario para la rápida transferencia de datos y voz de un lugar a otro. Estos dispositivos, diseñados para su interacción con una infraestructura existente, pueden administrarse de forma centralizada

y proporcionan transferencia simultánea de datos, voz y vídeo; al tiempo que ofrecen un método flexible y eficiente de optimizar las capacidades de la red corporativa.

Por otro lado, la gama de switches Cisco Catalyst Express 500, que llegó al mercado a mediados del mes de septiembre, asiste a la organización en la obtención de un mayor control sobre la forma en la que las personas se comunican e intercambian información. Además, mediante inteligencia integrada, estas propuestas pueden implementar aplicaciones y dispositivos con facilidad, ya sea a través de una PDA, un teléfono IP o un PC. Sin olvidar que con una solución Catalyst resulta sencillo implementar nuevos servicios en el futuro, como comunicaciones IP y dispositivos inalámbricos. “Nuestra oferta Catalyst Express 500 destaca por su simplicidad, y por sus notables funcionalidades de seguridad”, matiza Massa.

También capaces de optimizar las particularidades de las pymes son las soluciones inalámbricas Aironet, y los productos específicos de seguridad de la firma. Con respecto a estos últimos, destacan propuestas específicas con una única funcionalidad, como los firewalls PIX o las soluciones IDS-IPS; y alternativas que combinan diferentes aspectos de seguridad, como los productos ASA, que aúnan funciona-

lidades firewall, VPN e IDS-IPS, y que se adaptan mejor a las necesidades de las empresas medianas.

Finalmente, hay que resaltar la aportación de Call Manager Express, “versión de software que se instala en los routers de servicios integrados para convertirlos en una centralita IP con terminales de teléfonos inalámbricos y de sobremesa con una única infraestructura de red IP”, sostiene el director comercial para pymes de Cisco.

#### CISCO SMB SUPPORT ASSISTANT

Para ayudar a una pyme a obtener todo el potencial de su red, resulta conveniente contar con un ingeniero de Cisco que pueda mantenerla en un estado óptimo de funcionamiento. Cisco SMB Support Assistant ofrece esta clase de servicio a través de herramientas on line y soporte técnico. Además, el distribuidor local de Cisco puede ofrecer servicios adicionales y soporte posventa.

“Dentro de nuestra propuesta de servicios de soporte y mantenimiento, incluimos herramientas de soporte on site, proponemos la sustitución de hardware en un día y concedemos la posibilidad de solicitar un equipo alternativo para ese periodo. Asimismo, aportamos servicios de reparación en el software del equipo, y acceso gratuito a actualizaciones de software y corrección de errores”, espeta Massa.

## Cisco Business Communications Solutions

Propuesta para pymes que incluye:

#### ■ Soluciones específicas para este entorno:

- routers de servicios integrados
- switches Catalyst Express 500
- soluciones inalámbricas Aironet
- productos específicos de seguridad (firewall, IDS-IPS...)
- soluciones de telefonía IP como Call Manager Express

#### ■ Servicios de soporte y mantenimiento

(Cisco SMB Support Assistant)

#### ■ Servicios de financiación

(Easy Renting)

### Secure Network Foundation, o Solución de red sólida y segura de Cisco:

- propuesta que Cisco presenta como solución de infraestructura de red segura, para construir una base sólida, sencilla y segura para las pymes



# El canal de seguridad



## LOS ESPECIALISTAS

Llegados a este punto, tenemos que dedicar espacio a la piedra angular de Cisco Systems para la comercialización de su propuesta en el entorno de la seguridad: su canal. Sin él, la compañía fracasaría en su intento de proporcionar a los clientes una infraestructura de red segura. Pero, si el canal es una pieza básica en el modelo de Cisco, qué hace que la propuesta de esta compañía sea tan atractiva para sus partners. “Para Cisco, la seguridad es innata a la red, así que en cada proyecto para construir una infraestructura de red, la seguridad tiene que estar incluida”, explica **Miquel Feliu, responsable de desarrollo de negocio de canal de Cisco Systems**. “De modo que, si un partner de Cisco está implantando una solución de red y no está incluyendo la seguridad en ella, está perdiendo una oportunidad de negocio y, además, no está ofreciendo el asesoramiento adecuado a su cliente”.

Las oportunidades que para un partner se derivan de la venta de soluciones de seguridad Cisco son múltiples, pues, al tiempo que cubre una necesidad real del cliente, desarrolla un negocio por el que puede diferenciarse frente a su competencia, aumenta sus ventas y obtiene mayores márgenes.

### SINÓNIMO DE GARANTÍA

Para ofrecer al mercado su propuesta de seguridad con las mayores garantías, el fabricante cuenta con dos especializaciones en dicha tecnología: VPN/Security y Security VPN/Firewall Express. Ambas proveen a los partners de formación en una tecnología específica que cubre preventas, desarrollo básico y soporte post-venta, con la diferencia de que la primera está dirigida a aquellos partners que atienden grandes cuentas y la segunda a aquellos otros que se ocupan del mercado de la pequeña y mediana empresa. Con ambas los partners obtienen un conocimiento a fondo de unos productos determinados y de sus aplicaciones, y se focalizan en la obtención de las habilidades necesarias para implementar y mantener esa solución. Cuando un partner

obtiene una de las especializaciones mencionadas logra ser percibido en el mercado como un experto en dicha tecnología. No sólo eso, sino que la especialización le otorga el conocimiento necesario para la integración con aplicaciones de software complementarias a la tecnología elegida. Por su parte, el cliente sabe que un partner especializado en tecnología Cisco es sinónimo de garantía.

El programa de especialización para partners de Cisco se actualiza constantemente, ya que la compañía se preocupa de revisar los requisitos necesarios para su obtención, dependiendo de las condiciones del mercado en cada momento.

### BENEFICIOS PARA EL PARTNER

Para obtener la especialización VPN/Security, el partner deberá contar con un responsable comercial, un técnico preventa y otro postventa, que hayan aprobado los exámenes necesarios. Para lograr VPN/Firewall Security Express, el partner tiene que disponer de un responsable comercial y un ingeniero de sistemas que también han de superar unas pruebas adaptadas al conocimiento necesario para el tamaño de empresas que deberán atender.

Una vez que el partner cuente con una de ellas, los beneficios que obtendrá son múltiples. Para empezar, se diferenciará de sus competidores; en segundo lugar habrá migrado hacia un negocio de valor añadido con márgenes más altos; como tercer beneficio aparecerá en el “localizador de partners” de Cisco; por último, contará con el apoyo de la fuerza de ventas de la firma, que recomienda preferentemente partners especializados. Sumados a todos estos beneficios, la posesión de una especialización concede al partner puntos para su certificación como Gold, Silver o Premier, así como acceso al laboratorio virtual y a equipos para realizar demos ante sus clientes.

Para motivar a los partners en la venta de soluciones de seguridad, Cisco cuenta con hasta tres programas que son los que detallamos a continuación:

### VPN Security:

- Unitronics Comunicaciones
- Telefónica Soluciones de Informática y Comunicaciones de España
- Getronics
- BT España
- Telindus
- Fujitsu ICL
- Dimension Data
- SATEC SA/CONVEX
- T-Systems ITC
- HP
- Soluziona
- NextiraOne
- Eurocomercial Informática y Comunicaciones
- Scorpion Networking Solutions
- Amper Medidata
- Avanzit Tecnología
- Telecomunicaciones Digitals
- Nexica
- Pronet Programación y Networking
- IBM
- Davinci Consulting

### Security VPN/Firewall Express

- Alhambra System
- Infogroup Sistemas

## LOS EVENTOS

Con el objetivo de seguir ahondando en la formación de sus partners, Cisco cuenta con hasta tres eventos dedicados al entorno de la seguridad. “**Challenge & Reward** es una reunión que organizamos trimestralmente tanto para los partners que participan en Challenge & Reward Seguridad como para los que lo hacen en Challenge & Reward Voz”, especifica Miquel Feliu. Con él se pretende que dichas empresas dispongan de las últimas herramientas técnicas y comerciales, así como de la información sobre las novedades de productos. Para ello, la compañía organiza demostraciones, presentaciones, etc.

El segundo evento en torno a dicha área recibe el nombre de **Senator Club**, y fue concebido

para los partners especializados de Cisco, con el fin de avanzarles las últimas novedades y tendencias en el entorno de seguridad.

El tercero y último de los escenarios es **Cisco Innovation Tour**, que, con una periodicidad anual, se desarrolla en distintos países de EMEA. “En el caso de España, a la última edición celebrada en junio asistieron un total de 500 participantes, entre clientes y partners, que pudieron acudir a las ponencias sobre seguridad y visitar a los expositores”, en palabras de Miquel Feliu, que anticipa que el tercer Cisco Innovation Tour se celebrará en el primer trimestre de 2006, y que, como novedad, contemplará también las competencias de Wireless y Telefonía IP.

## CHALLENGE & REWARD SEGURIDAD

Es el programa principal en esta área y fue diseñado para el desarrollo tanto comercial como técnico de los partners en el área de seguridad. Para lograrlo, Cisco les ofrece un plan de formación, acceso a laboratorio y a herramientas comerciales para la venta. Otras ventajas para los partners que forman parte del programa son: la obtención de un incentivo en forma de descuento y la ayuda directa de un channel account manager de Cisco.

“Para formar parte de este programa el requerimiento principal es conseguir la especialización en VPN/Security Express en 6 meses”, explica Miquel Feliu.

En la comunicación a los partners de la información relativa a Challenge & Reward, así como en el reclutamiento de los mismos, Cisco cuenta con la colaboración de sus mayoristas: Comstor, Diasa, Ingram Micro y Tech Data.

## OIP (OPPORTUNITY INCENTIVE PROGRAM)

El programa OIP ofrece incentivos económicos a aquellos partners que identifican, desarrollan y cierran una nueva oportunidad de negocio. Sin embargo, como explica Miquel Feliu, “dicha oportunidad tiene que encontrarse en el área que Cisco denomina ‘Commercial’, organizaciones de hasta 2.500 puestos de trabajo”. Eso sí, una vez identificada, el partner tiene que registrar dicha oportunidad en la web del programa. El incentivo económico consiste en un 6% de descuento, “que el partner decide si repercutir o no en la operación con su cliente, y que se mantiene para los siguientes proyectos que se ese partner realice en ese cliente”.

## VIP6 (VALUE INCENTIVE PROGRAM)

Este programa incentiva en forma de rebate las ventas realizadas por un partner en seguridad. En concreto, consiste en que el reseller vende durante seis meses y, si consigue una cifra de más de 100.000 dólares en productos de seguridad, recibe un rebate de entre un 7 a un 14% a posteriori de estas ventas.

Cisco también ha desarrollado dicho programa para las especializaciones de IP Communications, e IP Communications Express.



## PROGRAMAS

- **Challenge and Reward Seguridad**  
*Desarrollo comercial y técnico en seguridad para los partners*
- **OIP (Opportunity Incentive Program)**  
*Incentivos para los partners que identifican y cierran una operación*
- **VIP6 (Value Incentive Program)**  
*Bonificación de entre un 7 y un 14% por las ventas logradas*

## ESPECIALIZACIONES

- **VPN Security**  
*Especialización para partners que atienden proyectos de seguridad en la gran cuenta*
- **Security VPN/Firewall Express**  
*Especialización para partners que atienden proyectos de seguridad en la pyme*

## EVENTOS

- **Challenge and Reward**  
*Evento trimestral para ofrecer herramientas técnicas y comerciales*
- **Senator Club**  
*Dirigido a los partners de consultoría para avanzarles novedades*
- **Cisco Innovation Tour**  
*Encuentro anual con ponencias y área de exposición para clientes y partners*



Para más información contacte con su Cisco Account Channel Manager

# TCN

www.mcediciones.net/tcn

**Nº 280**

9 - 15 de noviembre de 2005

**DIRECTORA** Gemma Sahagún  
gsahagun@mcediciones.es

**REDACTORA JEFE** Silvia Torres  
storres@mcediciones.es

**JEFE DE SECCIÓN** Manuel Hernando  
mhernando@mcediciones.es

**REDACCIÓN** Mónica Marugán  
(monica.marugan@mcediciones.es)  
Paula Szerman  
(pszerman@mcediciones.es)

**DISEÑO** Eva Herrero  
eherrero@mcediciones.es

**FOTOGRAFÍA** Sebastián Romero Márquez  
rmarquez@mcediciones.es

**WEBMASTER** Eduard Couchez  
webmaster@mcediciones.es

**COLABORADORES** Manuel Navarro

**PUBLICIDAD INTERNACIONAL** Carmen Ruiz  
carmen.ruiz@mcediciones.es

**COMERCIALES** Esther García  
estherg@mcediciones.es  
Albert Albalat  
tcnbcn@mcediciones.es

**SECRETARIA PUBLICIDAD MADRID** Mar Morato  
Orense, 11. 28020 Madrid  
Teléfono: 91 417 05 13. Fax: 91 417 05 18  
morato@mcediciones.es

**SECRETARIA PUBLICIDAD BARCELONA** Montse Jiménez  
Paseo San Gervasio, 16-20  
08022 Barcelona  
Teléfono: 93 254 12 50. Fax: 93 254 12 61  
mjimenez@mcediciones.es

**DISTRIBUCIÓN Y SUSCRIPCIONES** Fernando García  
fgarcia@mcediciones.es  
Elena Delgado  
edelgado@mcediciones.es



**EDITORA GERENTE** Susana Cadena  
Jordi Fuertes

**ADMINISTRACIÓN** Paseo San Gervasio, 16-20.  
08022 Barcelona  
Tel.: 93 254 12 50. Fax: 93 254 12 60  
**OFICINA EN MADRID** c/ Orense 11, bajos. 28020 Madrid  
Tel.: 91 417 04 83. Fax: 91 417 04 84

**DISTRIBUYE** COEDIS S.L.  
Av. Barcelona, 225  
08750 Molins de Rei. Barcelona

**OFICINA EN MADRID** c/ Alcorcón, 9. Pol. Ind. Las Fronteras  
28850 Torrejón de Ardoz. Madrid

**IMPRESIÓN** Printone

Depósito legal: B-23190-99

"TCN" puede contener artículos licenciados por CMP Media Inc., dichos artículos han sido traducidos e impresos con el permiso de "Computer Reseller News".  
Copyright © 2002 CMP Media LLC Todos los derechos están reservados

**ARI** Asociación de Revistas de Información

Difusión controlada por



CISCO SYSTEMS

