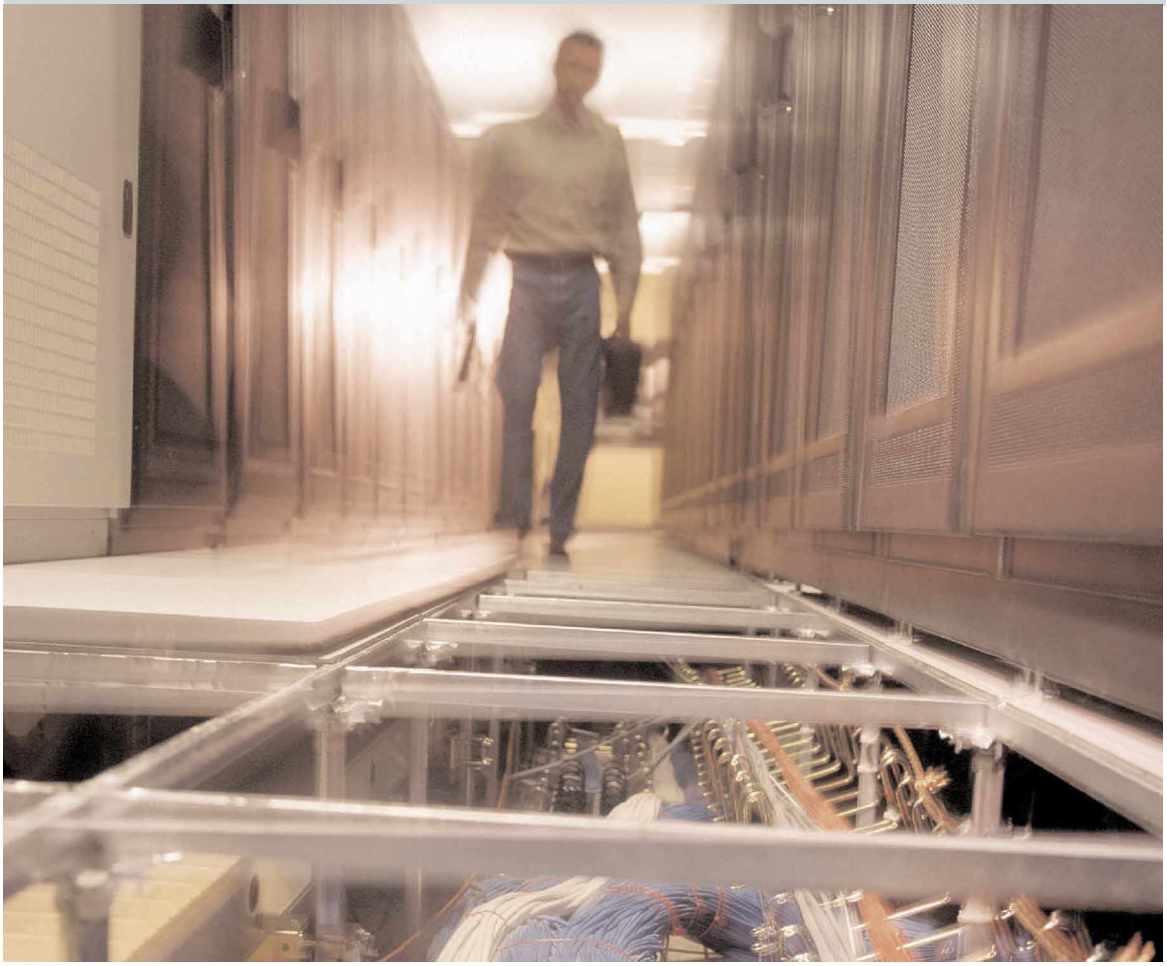
Guía de soluciones



SEGURIDAD DE REDES INTEGRADA DE CISCO: CONSTRUIR UNA RED AUTODEFENSIVA

"Las redes han evolucionado y han pasado de ser sistemas cerrados a sistemas más abiertos y sofisticados. En consecuencia,
las amenazas a la seguridad han aumentado de forma exponencial, tanto en el perímetro de la red como en su interior. Cisco ha respondido con una estrategia que integra los servicios de seguridad en la infraestructura de la red. Ésta proporciona un planteamiento completo, económico y flexible para proteger la red extendida de hoy en día".

Zeus Kerravala
Vicepresidente, Informática de empresa, infraestructura de aplicaciones para conexión de redes
y plataformas de software,
The Yankee Group

Cada día, las empresas con visión de futuro reinventan su forma de hacer negocios adoptando soluciones de red basadas en Internet. Los resultados: ventaja competitiva, nuevas fuentes de ingresos y procesos comerciales optimizados.

Cada vez son más las aplicaciones y los servicios empresariales esenciales que se despliegan en redes abiertas con conexiones numerosas a Internet. Si no se cuenta con políticas, procesos y productos de seguridad adecuados, la conectividad a Internet puede poner en peligro los mismos avances de productividad que hacen más rentables a las empresas de hoy y les permiten prestar servicio a una base de clientes más amplia y diversa.

La seguridad permite a las empresas ampliar con confianza su red a clientes, socios y trabajadores móviles/a distancia, con lo que se incrementan las fuentes de ingresos y se mejora la eficacia de los procesos comerciales y la productividad de los empleados.

En algunas industrias, la confidencialidad de los datos y la amenaza de litigios se ha convertido en un mandato gubernamental. Los proveedores de servicios de salud de EE.UU. deben cumplir con la Ley de Responsabilidad y Transferibilidad del Seguro de Salud (Health Insurance Portability and Accountability Act o HIPAA), los proveedores de servicios financieros de EE.UU. se rigen por la Ley Gramm-Leach-Bliley y las empresas del Reino Unido deben cumplir con los requisitos del informe Turnbull sobre control interno para las sociedades que cotizan en Bolsa, además de con la Ley de Protección de Datos de 1995.

Puesto que se transfiere información de carácter delicado a través de infraestructuras de redes públicas y privadas, es necesario contar con controles y políticas de seguridad para paliar el posible riesgo (que muestren la diligencia debida) con el fin de garantizar la protección de dicha información de acuerdo con políticas de privacidad de alto nivel y los requisitos de la normativa vigente.

LA VISIÓN DE CISCO

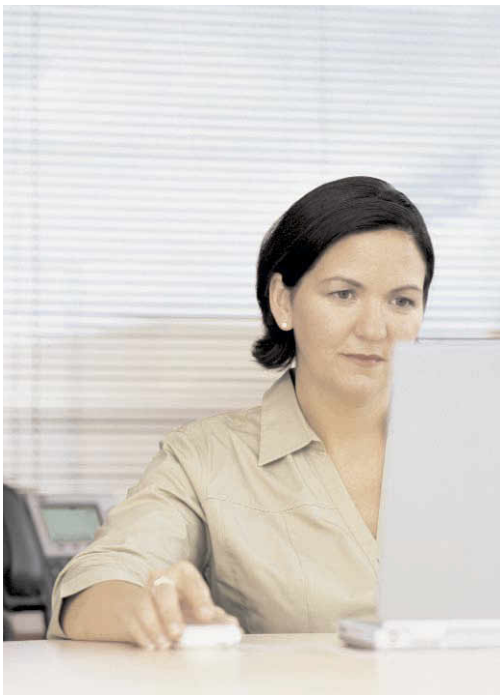
Cisco Systems® es un socio de confianza que faculta a sus clientes para que puedan desplegar aplicaciones y procesos esenciales para los negocios de manera segura en redes de información inteligentes y así les ayuda a aumentar su productividad y obtener una ventaja competitiva. Estas redes están integradas, son resistentes y adaptables. La confianza que se tiene al saber que los procesos comerciales y los recursos de información de la compañía están protegidos es un factor crítico a la hora de materializar enormes ganancias de productividad y un crecimiento dinámico.

Otros proveedores de seguridad pueden ofrecer productos puntuales que consiguen un nivel básico de seguridad para las redes IP. Por su parte, Cisco® ofrece los sistemas y servicios de seguridad de redes integrada avanzados necesarios para las redes empresariales con funciones cruciales.

Cisco continúa incorporando inteligencia en seguridad a la infraestructura de las redes, pues comprende que la seguridad no es un factor de última hora -sino que es fundamental para los procesos comerciales- y, en última instancia, para el éxito en los negocios.

CONSTRUIR LA RED AUTODEFENSIVA

La estrategia para construir la Red Autodefensiva de Cisco describe nuestra visión sobre los sistemas de seguridad. De la misma forma que la naturaleza de las amenazas contra las organizaciones está evolucionando, también debe hacerlo su posición de defensa. En el pasado, las amenazas procedentes de fuentes tanto externas como internas avanzaban de forma relativamente lenta y resultaba fácil defenderse de ellas. En el entorno actual, en el que los gusanos se propagan a través de Internet en todo el mundo en cuestión de minutos los sistemas de seguridad -y la propia red- deben reaccionar de manera inmediata.



La base de una Red Autodefensiva es la seguridad integrada: la seguridad que es intrínseca a todos los aspectos de una organización. Cada uno de los dispositivos de la red -desde los equipos de escritorio pasando por la red LAN y hasta la red WAN- desempeña un papel en la protección del entorno de la red a través de una defensa distribuida a nivel global. Esos sistemas ayudan a garantizar la confidencialidad de la información transmitida y a protegerla contra las amenazas tanto internas como externas, mientras que proporcionan a los administradores de la compañía el control del acceso a los recursos de la compañía. El planteamiento de Cisco sobre la seguridad ha evolucionado desde la oferta de productos puntuales hasta este planteamiento de seguridad integrada. La evolución continua de nuestra visión implica la incorporación de funciones de otros proveedores de seguridad. En la iniciativa de Control de acceso a la red de Cisco, por ejemplo, Cisco está trabajando con proveedores de productos antivirus para garantizar que los dispositivos infectados no puedan obtener acceso a la red.
Estas redes autodefensivas identificarán las amenazas, reaccionarán de forma apropiada según el nivel de gravedad, aislarán los servidores y equipos de escritorio infectados y reconfigurarán los recursos de la red en respuesta a un ataque.

La visión de Cisco sobre la Red Autodefensiva reúne conectividad segura, defensa contra amenazas y un sistema de administración de identidad y confianza con la capacidad de contención de la infección y aislamiento de dispositivos infectados en una misma solución.

ELEMENTOS CRUCIALES DE LA SEGURIDAD EN LA RED

Las soluciones de Seguridad de redes integrada de Cisco incorporan tres elementos que Cisco considera cruciales para una seguridad eficaz de la red.

Sistema de defensa contra amenazas
Las amenazas de hoy en día -tanto conocidas como desconocidas- son cada vez más destructivas y ocurren con más frecuencia que en el pasado. Las amenazas internas y externas, como los gusanos, ataques de denegación de servicio (DoS), ataques de intermediario, caballos de Troya, entre otros, tienen la capacidad de afectar de forma significativa a la rentabilidad de las empresas. El Sistema de defensa contra amenazas de Cisco proporciona una defensa sólida contra estos ataques conocidos y desconocidos.

Se requieren tecnologías de seguridad adecuadas junto con una inteligencia avanzada en la conexión de redes para poder defenderse con eficacia de estos ataques. Para una mayor eficacia, estas tecnologías deben implementarse en toda la red, en lugar de limitarse a productos o tecnologías puntuales, puesto que el origen de un ataque puede estar en cualquier parte y propagarse de forma instantánea a todos los recursos de la red. El Sistema de defensa contra amenazas de Cisco fortalece la seguridad en la infraestructura de red existente, añade seguridad completa en los puntos terminales (tanto en servidores como equipos de escritorio), e incorpora tecnologías de seguridad dedicada a los dispositivos y aparatos de conexión de redes, todo ello para defender de manera proactiva el negocio, las aplicaciones, los usuarios y la red. El Sistema de defensa contra amenazas protege a las empresas de interrupciones en sus operaciones, de la pérdida de ingresos y de su buena reputación.

El Sistema de defensa contra amenazas de Cisco comprende varias tecnologías y productos cruciales que posibilitan la seguridad integrada en routers, switches y aparatos: firewalls, sensores de protección contra intrusiones basados en la red, instrumentos de detección y técnicas de aislamiento del tráfico. La protección de puntos terminales es posible a través de Cisco Security Agent.

Sistema de conectividad segura

El incremento de la conectividad de redes conlleva un mayor riesgo de exposición.
A medida que las organizaciones adoptan el uso de Internet para su conectividad de redes internas, redes externas y para la conectividad de sus trabajadores a distancia, por ejemplo las conexiones "siempre activas" de banda ancha, se hace imprescindible mantener la seguridad, la integridad de los datos y la confidencialidad en estas conexiones.

Las conexiones LAN, consideradas tradicionalmente como redes de confianza ahora requieren también niveles de seguridad más elevados. De hecho, las amenazas internas son diez veces más perniciosas desde el punto de vista económico que las amenazas externas.
Mantener la confidencialidad y la integridad de los datos y la aplicaciones que atraviesan las redes LAN cableadas e inalámbricas debe ser una parte importante de las decisiones comerciales de una empresa.

El Sistema de conectividad segura de Cisco utiliza funciones de cifrado y autenticación que permiten el transporte seguro a través de redes que no son de confianza. A fin de proteger las aplicaciones de datos, voz y vídeo a través de medios cableados e inalámbricos, Cisco ofrece Seguridad IP (IPSec), Secure Sockets Layer (SSL), Secure Shell (SSH) y tecnologías VPN basadas en conmutación de etiquetas de protocolos múltiples (MPLS), además de completas funciones de seguridad incorporadas a las soluciones de telefonía IP inalámbrica de Cisco que garantizan la confidencialidad de todas las comunicaciones IP. Las soluciones de Cisco ofrecen conectividad confiable y flexible mediante la integración de enrutamiento dinámico, compatibilidad con numerosos protocolos y la más amplia variedad de opciones de conectividad de la industria.

Sistema de administración de identidad y confianza

Un Sistema de administración de identidad y confianza es crucial para las operaciones de e-business y sustenta la creación de cualquier red o sistema seguro. Conlleva el facilitar o denegar el acceso a aplicaciones comerciales y recursos disponibles en red de acuerdo con ciertos derechos y privilegios específicos del usuario.

El Sistema de administración de identidad y confianza de Cisco se centra en el control de admisión basado en la red. Tras confirmar la identidad de un usuario o dispositivo, así como su cumplimiento de la política de seguridad de la compañía, puede habilitarse el acceso a determinados recursos o partes de la red. La red es responsable de la identificación, autorización y cumplimiento. La solución de identidad y confianza de Cisco, que incluye Cisco Secure Access Control Server (ACS), protocolos de autenticación como 802.1X y funciones AAA (autenticación, autorización y contabilidad) en los switches y routers de Cisco, tiene la flexibilidad de proporcionar un elevado nivel de derechos de acceso y de crear zonas de cuarentena para los puntos terminales que presenten una no conformidad, además de la posibilidad de bloquear completamente todo acceso no autorizado.

SOLUCIONES DE SEGURIDAD INTEGRADA DE CISCO- UNA FAMILIA DE OFERTAS DE SEGURIDAD PARA LA RED

Los prestigiosos productos de seguridad y los servicios de entrega, asistencia y asesoramiento de Cisco proporcionan las soluciones de seguridad que requieren las empresas.

Firewall, VPN y protección contra intrusiones integrados-

Figura 1 Equipo de seguridad PIX de Cisco

Equipo de seguridad Serie Cisco PIX 500

El Equipo de seguridad Serie Cisco PIX® 500 (Figura 1) es el firewall más importante del mundo, que proporciona una confiabilidad, escalabilidad y conjunto de capacidades sin igual en la industria. Ofrecidos como una serie de equipos especializados y como un módulo integrado para los switches Catalyst® de Cisco, los equipos de seguridad PIX de Cisco presentan una arquitectura de seguridad híbrida innovadora -que incluye inspección de paquetes que conserva su información de estado y funciones VPN con IPSec integrada-. Los equipos de seguridad PIX de Cisco ofrecen los niveles más elevados de seguridad y rendimiento, y admiten más conexiones simultáneas que cualquier otro firewall, a una velocidad inigualable.

Routers de seguridad Cisco y switches Catalyst de Cisco

Cisco ha integrado directamente la seguridad en la infraestructura de la red por medio de funciones de seguridad mejoradas en los routers de Cisco y en los switches Catalyst de Cisco, lo que proporciona una flexibilidad y ahorro de costos sin igual para las instalaciones de seguridad. Al aprovechar estos dispositivos de red, las organizaciones pueden aplicar políticas de seguridad sofisticadas, de extremo a extremo, haciendo uso de su inversión en infraestructura de Cisco. El software Cisco IOS® que se ejecuta en routers Cisco y en switches Catalyst de Cisco incluye compatibilidad con VPN IPSec y MPLS con todas sus funciones, basados en estándares para la conectividad de sucursales y de acceso remoto. Los routers y switches Catalyst de Cisco incluyen además un robusto firewall con inspección de paquetes que conserva su información de estado y un sistema detección de intrusiones
(IDS), con capacidad para escalar el rendimiento por medio de módulos de aceleración tipo plug-in.
Y por último, los routers de Cisco y los switches Catalyst de Cisco son los mecanismos de control de acceso principales que permiten o desautorizan la conectividad de los puntos terminales a los recursos conectados en red.

IDS de Cisco

El IDS de Cisco ofrece protección contra intrusiones en tiempo real para el perímetro de la red, las redes externas y la cada vez más vulnerable red interna. El sistema utiliza sensores, los cuales son equipos de red de alta velocidad, que analizan paquetes individuales y detectan cualquier actividad sospechosa. Si el flujo de datos presenta una actividad no autorizada o un ataque a la red, los sensores pueden detectar la actividad indebida en tiempo real, enviar alarmas a un administrador y expulsar al atacante de la red.

Soluciones de seguridad de puntos terminales-

Cisco Security Agent

Cisco Security Agent (CSA) es un software de protección de puntos terminales que reside en equipos personales y servidores. CSA supera a las soluciones convencionales identificando e impidiendo comportamientos maliciosos antes de que se produzcan, eliminando así los riesgos potenciales de seguridad conocidos y desconocidos ("Día cero") como los gusanos que se propagan a través de Internet.

Figura 2 Concentradores Serie Cisco VPN 3000

Soluciones VPN de acceso remoto de Cisco-

Concentrador de Serie Cisco VPN 3000

Los concentradores de la serie Cisco VPN 3000 (Figura 2) son plataformas VPN de acceso remoto que combinan alta disponibilidad, alto rendimiento y escalabilidad con las técnicas de autenticación y cifrado más avanzadas existentes. El uso de la tecnología VPN más avanzada reduce enormemente el costo de las comunicaciones. Los concentradores de la serie Cisco VPN 3000 son las únicas
plataformas escalables que ofrecen componentes ampliables por el cliente y que se pueden intercambiar sobre el terreno.
Estos componentes, denominados módulos de Procesamiento de cifrado escalable (SEP), permiten a los usuarios agregar capacidad y caudal de procesamiento con facilidad. La flexibilidad de la serie Cisco VPN 3000 permite a la vez la terminación de túneles VPN con IPSec y SSL para lograr una mayor flexibilidad y reducción del costo de adquisición.

Soluciones de cliente VPN de Cisco-

Cliente VPN de Cisco

El Cliente VPN de Cisco posibilita la conectividad segura para VPN de acceso remoto, e incluye la compatibilidad con aplicaciones de comercio electrónico, usuarios móviles y trabajo a distancia. Compatible con los sistemas operativos Windows, Linux, Solaris y Macintosh, el Cliente VPN de Cisco ofrece una implementación completa de las normas IPSec, incluidos el Estándar de cifrado de datos (DES) y DES triple (3DES), cifrado AES y la autenticación por medio de certificados digitales, contraseñas de un solo uso y claves previamente compartidas, RADIUS, Dominio NT, Active Directory/Kerberos y autorización LDAP. El Cliente VPN de Cisco es compatible con la mayoría de las plataformas de cabecera de red de Cisco, incluidos los concentradores Cisco VPN 3000, firewalls PIX de Cisco y todos los routers habilitados con VPN de Cisco.

Soluciones de administración de contenido de Cisco-

Aceleración SSL de Cisco

Cisco ofrece las soluciones más completas y de más alto rendimiento de la industria para dar soporte a redes internas, redes externas y aplicaciones en Internet basadas en SSL. Las soluciones de Cisco optimizan las transacciones mediante SSL para liberar la capacidad del servidor, escalar el rendimiento del sitio, incrementar la confiabilidad de las transacciones seguras y simplificar la administración de certificados de usuario, reduciendo tanto los gastos operativos como de capital.

Administración de acceso a contenidos y filtrado de contenido

Cisco ofrece soluciones para la administración del acceso al contenido en el extremo de la red, lo que ofrece a empresas y escuelas opciones dirigidas a bloquear contenido objetable en la Web y filtrar las direcciones URL. Las ventajas: mejor administración del acceso a la Web y reducción de la exposición a responsabilidades.

Soluciones de administración de identidad y confianza de Cisco-

Servidor de control de acceso seguro de Cisco

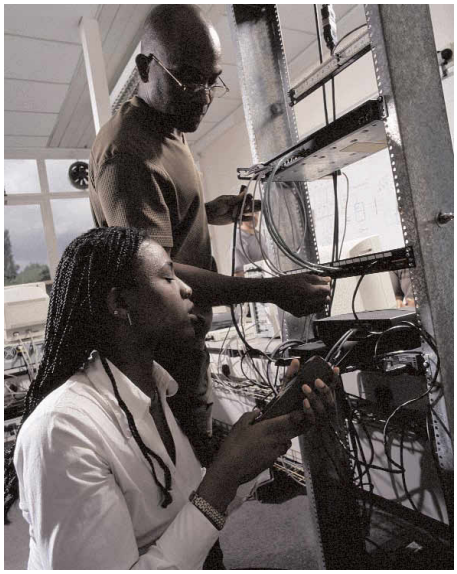
Cisco Secure ACS es un servidor de control de acceso altamente escalable, de alto rendimiento que funciona como sistema de servidor RADIUS o TACACS+ centralizado. Controla las funciones de AAA para los usuarios que acceden a los recursos de la compañía a través de una red. Al usar Cisco Secure ACS, los administradores de red pueden controlar el acceso de los usuarios a la red, autorizar diferentes servicios de red para usuarios o grupos de usuarios y mantener un registro de contabilidad de todas las acciones realizadas por los usuarios en la red. Asimismo, los administradores de la red pueden usar la misma estructura de AAA para gestionar (mediante TACACS+) las tareas administrativas y los grupos, y controlar cómo cambian, acceden a la red y la configuran a nivel interno.

Como motor de creación de políticas de la solución de Control de admisión a la red de Cisco, Cisco Secure ACS proporciona la inteligencia y el control que sustenta la política de seguridad de una organización.

Soluciones de administración de seguridad de Cisco-

Administración integrada a través de la Solución de administración de seguridad/VPN de Cisco (VMS)

CiscoWorks VMS ofrece un planteamiento innovador con respecto a la administración de infraestructuras a nivel de toda la empresa.
Esta solución mejorada proporciona una mayor seguridad en la red mediante una automatización que simplifica y mejora la administración de firewalls remotos. Permite realizar implementaciones y actualizaciones más rápidamente a través de una interfaz en la Web sencilla y fácil de usar. Conduce a incrementos de productividad y disminuye el costo total de adquisición mediante una inteligencia que permite seguir y cumplir los procesos y políticas comerciales, evitando interrupciones innecesarias en el negocio. CiscoWorks VMS se amplía ahora con respecto a la versión más básica que admite hasta 5 dispositivos, a una versión de gama alta que admite más de 1000 routers de seguridad IOS de Cisco. CiscoWorks VMS permite además una mayor productividad y un excelente rendimiento de la inversión por medio de su integración con otras herramientas de CiscoWorks, las cuales administran la infraestructura de la red.



CISCO OFRECE LOS SIGUIENTES SERVICIOS DE SEGURIDAD DE LA RED:

· Servicios de implementación de Cisco Security Agent
· Revisión de seguridad de telefonía IP
· Desarrollo del diseño de seguridad de la red
· Revisión del diseño de seguridad de la red
· Ingeniería de implementación de seguridad en la red
· Revisión del plan de implementación de seguridad en la red
· Optimización de seguridad en la red
· Valoración de posición de seguridad

Administración de dispositivos únicos y múltiples
Cada plataforma ofrece su propia interfaz gráfica del usuario (GUI) inteligente para la administración de un solo dispositivo. La productividad y el costo total de adquisición mejoran gracias al uso de interfaces gráficas basadas en la Web de fácil uso. CiscoWorks VMS también puede utilizarse para la administración de varios dispositivos.

Soluciones de administración de información de seguridad CiscoWorks (SIMS)

Diseñadas para redes extensas, CiscoWorks SIMS recopila y analiza eventos de seguridad de los Sistemas de detección de intrusiones, firewalls, sistemas operativos, aplicaciones y dispositivos antivirus. Esta información de seguridad se correlaciona estadísticamente, se evalúa de acuerdo con normas de seguridad definidas y se presenta a los administradores en tiempo real en función de su prioridad en un formato en el que se pueda trabajar. CiscoWorks SIMS incluye funciones de diversos proveedores para las soluciones de seguridad de red integradas de Cisco. Sus galardonadas funciones están basadas en las tecnologías de netForensic que ayudan a las organizaciones a proteger sus avances de productividad y a reducir sus costos operativos.

SERVICIO Y ASISTENCIA DE CISCO

El modelo Cisco de servicio y asistencia se basa en el conocimiento de que aprovechar el poder que brinda Internet no sólo acelera la resolución de problemas de conexión de redes, sino que además hace posible el acceso por parte de los clientes a información crucial con rapidez, para adquirir conocimientos y para mejorar de manera proactiva el rendimiento general de la red.

Cisco.com es la base de un paquete de aplicaciones conectadas en red interactivas que ofrecen un acceso abierto e inmediato a la información, los recursos y sistemas de Cisco. A través de Cisco.com, los clientes directos y partners tienen acceso a numerosas aplicaciones como las de Asistencia técnica en Internet de Cisco (ITS), las cuales proporcionan soluciones completas en línea. Para ayudar a conseguir el máximo tiempo de actividad en la red, la asistencia técnica está disponible las veinticuatro horas del día a través de los ingenieros de redes del Centro de Asistencia Técnica de Cisco (TAC). Para obtener más información, visite:

http://www.cisco.com/tac

Servicios Avanzados de Cisco para seguridad en la red

Los consultores de Servicios Avanzados de Cisco poseen certificaciones CCIE® y CISSP a nivel experto y cuentan con experiencia en la planificación, diseño, implementación y optimización de infraestructuras de seguridad de red en importantes empresas comerciales y organizaciones gubernamentales.

Planificación y valoración. Cisco puede proporcionarle una evaluación completa de la posición de seguridad de la red de su organización. La Valoración de posición de seguridad de Cisco, realizada por expertos en seguridad que cuentan con amplia experiencia práctica, proporciona una instantánea del estado de seguridad de su red, mediante la realización de una evaluación minuciosa de sus dispositivos de red, servidores, equipos de escritorio y bases de datos. Los expertos de Cisco analizan la seguridad de su red con respecto a las mejores prácticas de la industria e identifican puntos vulnerables que podrían suponer una amenaza para su negocio. En función de un análisis pormenorizado, Cisco ofrece recomendaciones sobre cómo mejorar la seguridad general de la red y establece prioridades para las acciones correctivas.

Diseño. Cisco puede trabajar con usted para diseñar una red de autodefensa sólida. Valiéndose de un planteamiento minucioso basado en la arquitectura, los expertos de Cisco pueden ayudarle a crear una defensa de varios niveles contra ataques dirigidos por hackers, virus y gusanos. Cisco puede recomendar mejoras a su diseño de seguridad existente, incluyendo la topología de la red, colocación de dispositivos y conectividad. Considerando todos los aspectos de la seguridad de la red, como la capacidad de ampliación, el rendimiento y la capacidad de administración, Cisco puede recomendar configuraciones de protocolos, políticas y funciones para lograr una protección superior contra las amenazas.

Implementación. Una red de autodefensa no sólo debe diseñarse de forma estratégica, sino que es necesario desplegarla, configurarla e integrarla con sumo cuidado en la infraestructura de la red. Una vez establecido el diseño de la solución de seguridad, los ingenieros de Cisco pueden prestar asistencia a su equipo a lo largo de las tareas de implementación y ayudarle a integrar una nueva solución en el entorno de producción. Al reforzar la capacidad de su equipo para cumplir programas muy exigentes mientras se minimizan los costosos trastornos en la infraestructura, los ingenieros de Cisco pueden ofrecer la experiencia necesaria para desplegar, integrar y administrar la solución de seguridad.

Optimización. Una vez que haya diseñado y desplegado con éxito sus soluciones de seguridad, la infraestructura de la red estará lista para admitir las mayores demandas que surjan como consecuencia de cambios en la dinámica del negocio o del incremento de requisitos de la red. A medida que cambian las condiciones de la red, los ingenieros de Cisco colaboran con usted para realizar comprobaciones de optimización para ayudar a garantizar que la infraestructura de seguridad de la red continúe cumpliendo los requisitos de rendimiento.

Servicios de contratación externa de Cisco

Soluciones de servicios de seguridad administrados de Cisco

Para permitir a los proveedores de servicios aprovechar la creciente demanda de servicios administrados y servicios VPN seguros, Cisco cuenta con una extensa oferta para una introducción de servicios rápida y económica. Los servicios VPN administrados basados en IPSec, MPLS o en ambos permiten a los proveedores incrementar sus servicios de conectividad existentes con opciones de acceso remoto y de sitio a sitio, además de ofrecer servicios de valor añadido para telefonía IP, comercio electrónico, administración de la cadena de suministro,

y suministro de contenido. Los servicios de seguridad administrados, como firewall administrado y detección de intrusiones administrada, representan ofertas de valor añadido que pueden suministrarse unidos a otros servicios.

Tanto si ofrece servicios de VPN administrada, servicios de seguridad administrados, o ambos, podrá aprovechar las capacidades de los routers de Cisco y los switches Catalyst de Cisco que utiliza actualmente para obtener conectividad. Al hacer uso de su inversión actual, se minimizan los costos de despliegue y se maximizan las oportunidades de obtener nuevos canales de ingresos.

El programa Cisco Powered Network

Los proveedores de servicio que exhiben el símbolo Cisco Powered Network comunican información sobre sus servicios. Indican que se han ganado el derecho de exhibir este símbolo gracias al mantenimiento de unos niveles elevados en la calidad de su red y a la creación de servicios con equipos de Cisco -los mismos equipos por los que viaja prácticamente todo el tráfico de Internet actual-. Los servicios que prestan estos proveedores son confiables y seguros.

Partners de Cisco

El Programa de especialización en seguridad de Cisco reconoce a los partners de Cisco que han alcanzado las aptitudes necesarias para vender, diseñar, instalar y ofrecer asistencia para las soluciones de seguridad de redes de Cisco para los clientes. A medida que se van adoptando rápidamente soluciones comerciales en Internet, los partners con especialización en seguridad de Cisco pueden satisfacer la creciente demanda de servicios cruciales de implementación de seguridad y asistencia.

Servicios de capacitación de Cisco

Certificaciones de seguridad de Cisco

Las certificaciones de seguridad de Cisco proporcionan a individuos y organizaciones una métrica que les permite validar las aptitudes y competencias de profesionales de seguridad, por medio de la mejor capacitación y los mejores exámenes de su clase. El CCSP™ y las tres certificaciones enfocadas -Especialista en VPN de Cisco, Especialista en firewall de Cisco y Especialista en IDS de Cisco- satisfacen la demanda de la industria de proporcionar una vía profesional de certificación en el mercado de seguridad de TI. La certificación CCSP ayuda a garantizar que su personal implemente de forma satisfactoria soluciones de seguridad completas, de extremo a extremo.

Partners de aprendizaje de Cisco autorizados con enfoque en seguridad

Muchos partners de aprendizaje de Cisco autorizados de todo el mundo se centran en la capacitación en seguridad de Cisco ofreciendo cursos, laboratorios a distancia, material autodidáctico y otros recursos sobre las más recientes tecnologías. Entre éstas cabe mencionar los Firewalls PIX avanzados de Cisco, el Sistema de detección de intrusiones seguro de Cisco, la Implementación de diseño SAFE de Cisco y la Administración de seguridad en la red de Cisco. Puede utilizar el buscador de capacitación "Learning Locator" o consultar información sobre cursos, fechas de exámenes y una lista detallada de partners enfocados en seguridad en:

http://www.cisco.com/go/training

Ecosistema de seguridad de Cisco

Los productos, las tecnologías y los servicios de seguridad de la cartera de Cisco son elementos fundamentales de una solución de seguridad en la red. Un enfoque completo de la seguridad de la red debe incorporar también otras áreas -crear un "ecosistema de seguridad" que aproveche plenamente las ventajas ofrecidas por la línea de productos de Cisco-. Este ecosistema incluye varios elementos importantes, como los productos de terceros interoperativos, servicios de implementación, asistencia al cliente y oferta de servicios compatibles.

El Programa para partners de seguridad AVVID de Cisco es un programa de pruebas y marketing conjunto que valida la interoperabilidad de soluciones de seguridad de terceros complementarias a los productos de Cisco. El programa perfecciona productos independientes convirtiéndolos en soluciones de seguridad más eficientes y ofrece implementaciones de seguridad probadas y de confianza a los clientes de Cisco.

Resumen

Cisco-Construir su Red Autodefensiva

La visión de seguridad Cisco -facultar a los clientes de Cisco para que mejoren de forma segura su productividad- es lo que impulsa el compromiso de Cisco con la seguridad de su red y su éxito a largo plazo.

En la actualidad, Cisco ofrece soluciones de seguridad integrada que hacen posible una interconexión segura incorporando funciones de seguridad con gran riqueza de características en la infraestructura de Cisco y proporcionando numerosos equipos, software y servicios de asesoramiento específicos a la seguridad.

Las soluciones de seguridad de Cisco permiten a su negocio aprovechar de manera eficiente en términos de costo la economía de Internet con la confianza que necesita para explorar la siguiente generación de oportunidades y el crecimiento explosivo que brindan.

Para obtener más información sobre la seguridad integrada de Cisco y cómo construir una Red Autodefensiva, visite:

http://www.cisco.com/go/security
http://www.cisco.com/selfdefend
http://www.cisco.com/securitynow

PARA OBTENER MAS **INFORMACION**

Cisco Systems Argentina / Bolivia / Paraguay y Uruguay
Ing. Butty 240 - piso 17 - Capital Federal. (C1001ABF) - Argentina
Argentina:
0810-444-24726
Paraguay / Uruguay / Bolivia
+54-11-41321100 Ext. 0115
www.cisco.com.ar

Cisco Systems Brasil
Centro Empresarial Nações Unidas - CENU
Av. das Nações Unidas, 12901 - 26º e 18º andares
Torre Oeste São Paulo - SP - Cep: 04578-000
0800 702 4726
www.cisco.com/br

Cisco Systems Chile
Edificio World Trade Center, Torre Costanera
Av. Nva. Tajamar 555
Santiago - Chile.
800 52 2000
www.cisco.com/cl

Cisco Systems Colombia
Carrera 7 No. 71-21. Torre A. Piso 17
Bogotá, Colombia.
018009154303 Ext. 7182506
www.cisco.com/co

Cisco Systems Costa Rica
Centro Corporativo Plaza Roble
Edificio Los Balcones, Primer Nivel
San José, Costa Rica
0800-012-0118 ext. 2653
www.cisco.com/cr

Cisco Systems Ecuador
18776852773 Ext. 7182506

Cisco Systems Panamá
Edificio World Trade Center
Piso 17, Of 1701 Area Comercial, Marbella
Panamá
001-800-507-1286 Ext. 7182653
www.cisco.com/pa

Cisco Systems México
Paseo de Tamarindos 400A, Piso 30
Bosques de las Lomas, México.
001-800-667-0832
Mexico North Ext. 7186297
Mexico DF Ext 7186234
Mexico West Ext 7186235
Mexico South Ext 7182642
www.cisco.com/mx

Cisco Systems Perú
Av. Victor Andrés Belaunde 147, Vía Principal 123
Edificio Real Uno, piso 13
San Isidro, Perú.
+511 215-5117
www.cisco.com/pe

Cisco Systems Puerto Rico
Westernbank Plaza
268 Ave Munoz Rivera, Suite 2300
San Juan, PR 00918
Puerto Rico.
787 620 1888
Bermuda
1-877-841-6599 Ext 6214
Rep. Dominicana
1-888-156-1464 Ext 6214
www.cisco.com/pr

Cisco Systems Venezuela
Av. La Estancia, Centro Banaven,
Torre C, piso 7. Chuao.
0-800-100-4767 ext. 7182506/ 7182649
www.cisco.com/ve

US Toll free
1-800-667-0832
Phone USA: 1-800-493-9697

Cisco Systems cuenta con más de 200 oficinas en distintos paises y regiones. Direcciones, teléfonos y números de fax pueden ser encontrados en el siguiente site: **www.cisco.com/go/offices**

Alemania · Arabia Saudita · Argentina · Australia · Austria · Bélgica · Brasil · Bulgaria · Canadá · Chile · China PRC · Colombia · Corea · Costa Rica · Croacia · Dinamarca · Dubai, UAE · Escocia · Eslovaquia · Eslovenia · España · Estados Unidos · Filipinas · Finlandia · Francia · Grecia · Hong Kong SAR · Hungría · India · Indonesia · Irlanda · Israel · Italia · Japón · Luxemburgo · Malasia · México · Nueva Zelanda · Noruega · Países Bajos · Perú · Polonia · Portugal · Puerto Rico · Reino Unido · República Checa · Rumania · Rusia · Singapur · Sudáfrica · Suecia · Suiza · Tailandia · Taiwán · Turquía · Ucrania · Venezuela · Vietnam · Zimbabwe

N2/KW/LW5530 01/04