INFORME TÉCNICO

LAS CINCO CONSIDERACIONES DE SEGURIDAD PRIORITARIAS DE LAS MEDIANAS Y PEQUEÑAS EMPRESAS

Cisco ofrece redes de autodefensa diseñadas específicamente para medianas y pequeñas empresas.

RESUMEN

Las medianas y pequeñas empresas utilizan Internet y aplicaciones de red para acceder a nuevos clientes y prestar servicio a los clientes existentes de forma más eficaz. Al mismo tiempo, las nuevas amenazas contra la seguridad y la legislación incrementan la presión sobre las redes de las empresas para que ofrezcan seguridad y confiabilidad. Cisco® ofrece soluciones de seguridad integradas, completas y accesibles, diseñadas específicamente para las medianas y pequeñas empresas, que ayudan a garantizar la continuidad del negocio, a mantener la privacidad de los clientes y reducir los costos operativos. Las empresas pueden dedicar con toda confianza más tiempo a sus negocios y menos tiempo a los temas de seguridad en la red.

DESAFÍOS PARA LOS NEGOCIOS

El entorno empresarial actual de gran competitividad a nivel mundial hace que las medianas y pequeñas empresas centren su atención en ampliar sus negocios y mejorar la satisfacción del cliente, controlando a la vez sus costos. Afortunadamente, Internet y las aplicaciones de red han igualado las condiciones del juego. Las medianas y pequeñas empresas utilizan sus redes para ampliar su participación de mercado y comunicarse con sus clientes y partners de una forma rápida y económica. No obstante, la rapidez y agilidad que proporcionan las aplicaciones de e-business son un arma de doble filo: el acceso puede a su vez abrir la puerta a violaciones de seguridad que acarrean un elevado costo para las empresas. Ahora más que nunca es importante contar con redes confiables, seguras y disponibles.

CONSIDERACIONES DE SEGURIDAD

Según estudios recientes, la seguridad es el mayor desafío al que se enfrentan las medianas y pequeñas empresas. Las amenazas contra la seguridad en constante evolución, procedentes tanto del interior como del exterior de la red empresarial, pueden causar estragos en las operaciones comerciales, afectando a la rentabilidad de la empresa y la satisfacción del cliente. Además, las medianas y pequeñas empresas deben cumplir la nueva normativa y legislación creada para proteger la privacidad de los consumidores y garantizar la seguridad de la información electrónica.

Consideración de seguridad nº 1 - Gusanos y virus

Los gusanos y virus informáticos siguen siendo la amenaza más común contra la seguridad, con el 75 por ciento de las medianas y pequeñas empresas afectadas al menos por un virus al año*. Los gusanos y virus tienen un efecto devastador sobre la continuidad de las operaciones comerciales y sobre su rendimiento. Son cada vez más inteligentes y destructivos, y se propagan con más rapidez que nunca, pudiendo infectar a toda una oficina en cuestión de segundos. La actualización de los equipos infectados tarda mucho más tiempo. Los resultados catastróficos se concretan en la pérdida de pedidos, corrupción de las bases de datos y exasperación de los clientes. Mientras las empresas luchan por actualizar sus equipos con los sistemas operativos y software antivirus más recientes, los nuevos virus pueden penetrar en sus sistemas defensivos cualquier día de la semana. Mientras tanto, los empleados propagan virus y spyware accediendo a sitios web maliciosos de manera inadvertida o al descargar material poco confiable o abrir archivos maliciosos adjuntos en mensajes de correo electrónico. De forma no intencionada, se da paso a estos ataques al interior de la organización, que pueden provocar pérdidas financieras significativas. Los sistemas de seguridad deben detectar y repeler gusanos, virus y spyware en todos los puntos de la red.

Consideración de seguridad nº 2 - Robo de información

Actualmente el robo de información es un negocio muy lucrativo. Los astutos hackers acceden ilegalmente a las redes de las empresas con la intención de robar números de tarjetas de crédito o de identidad con fines lucrativos. Las medianas y pequeñas empresas están en peligro porque se las considera un objetivo más fácil que las grandes empresas. La protección del perímetro de la red es un buen comienzo, pero no es suficiente, ya que muchos robos de información se han llevado a cabo gracias a la ayuda de una persona de confianza que trabajaba desde dentro, por ejemplo, un empleado o contratista.

* Maritz Research, 2005

El robo de información puede ser muy costoso para las medianas y pequeñas empresas, ya que éstas dependen de la satisfacción de los clientes y de la buena reputación para el crecimiento de su negocio. Las empresas que no protegen adecuadamente su información podrían ser objeto de publicidad negativa, sanciones gubernamentales e incluso demandas judiciales. Por ejemplo, la nueva legislación sobre protección del consumidor promulgada en California requiere que las empresas que sospechen que ha habido un acceso no autorizado a información de sus clientes notifiquen a TODOS sus clientes. Toda estrategia de seguridad debe prevenir el robo de información de carácter confidencial tanto dentro como fuera del negocio.

Consideración de seguridad nº 3 - Disponibilidad del negocio

Los gusanos y virus informáticos pueden afectar drásticamente a la confiabilidad de los recursos de la red, lo cual puede a su vez afectar a la capacidad del negocio para responder rápidamente a sus clientes; sin embargo, los virus y gusanos no son la única amenaza para la disponibilidad del negocio. Puesto que las redes son tan cruciales para el desempeño diario de las operaciones comerciales, los terroristas del ciberespacio han comenzado a atacar a las empresas utilizando el chantaje, amenazándolas con sabotear sus sitios web y operaciones de comercio electrónico a menos que acaten sus exigencias. Estos ataques de denegación de servicio (DoS) envían un gran volumen de tráfico a un elemento imprescindible de la red, provocando fallas o impidiendo el paso del tráfico legítimo. Una vez más, los resultados son desastrosos: se pierden datos y pedidos y no se responde a las peticiones de los clientes. Si estos ataques pasan al dominio público, la credibilidad de la compañía se ve mermada. Aunque gran parte de la publicidad en torno a los bloqueos por DoS se ha centrado en grandes bancos y compañías de Global 500, las medianas y pequeñas empresas no son inmunes a estos ataques. Se las considera menos preparadas para reaccionar ante los ataques que las grandes empresas.

Existen otros tipos de ataque menos dramáticos pero más probables que amenazan a la disponibilidad de las medianas y pequeñas empresas y, en consecuencia, a su rentabilidad y la satisfacción del cliente. Por ejemplo, un ataque con robo de recursos transgrede las redes y los equipos informáticos, utilizándolos para el uso compartido ilegal de archivos, música, películas o software. Con frecuencia, las empresas no son conscientes de que se está produciendo una infracción de seguridad. Entretanto, sus equipos y redes funcionan con lentitud a la hora de responder a los clientes, y su participación inadvertida en el uso compartido ilegal de archivos las hace vulnerables a demandas judiciales.

Consideración de seguridad nº 4 - Lo desconocido

Con cada nuevo avance en informática y comunicaciones, los hackers malintencionados encuentran nuevas formas de explotar los puntos vulnerables de la tecnología para su provecho o para hacer daño. Las nuevas versiones de hardware o software presentan una nueva oportunidad. La conexión de redes de punto a punto y la mensajería de Internet (IM) eran aún aplicaciones relativamente nuevas cuando sus usuarios fueron atacados por código malicioso escrito específicamente para ellas. Ahora los teléfonos móviles son objetivo de los virus. Nadie sabe de dónde vendrá la próxima amenaza, pero la mejor defensa es la que permita adaptarse fácilmente a las futuras amenazas sin provocar la propia ruina.

Consideración de seguridad nº 5 - Legislación sobre seguridad

Paralelamente a estas amenazas maliciosas contra la seguridad, la nueva legislación y normativa exige a las medianas y pequeñas empresas que protejan la integridad y la privacidad de la información que se les ha confiado. La Unión Europea y muchos países a título individual cuentan con legislación que regula la protección de los datos personales depositados en las organizaciones. Algunos países han redactado también otras leyes para regular información específica, como la relacionada con la atención médica y la salud. Por ejemplo, en los Estados Unidos, la Ley de Responsabilidad y Transferibilidad del Seguro de Salud (HIPAA o Health Insurance Portability and Accountability Act) requiere que las organizaciones de atención médica, incluidas las consultas médicas, implementen medidas de protección para garantizar la privacidad de la información de salud e impida su acceso no autorizado. La responsabilidad recae en las empresas para que cumplan con la legislación y la normativa que se aplica a sus negocios y mercados específicos. Desgraciadamente, muchas empresas se dan cuenta de que sus recursos no dan para tanto. Aun así, los clientes quieren garantías de que la información que han confiado a las empresas se mantenga confidencial.

Todas las empresas deben tomar medidas para proteger la infraestructura de sus negocios, pero las medianas y pequeñas empresas en particular necesitan soluciones sencillas, accesibles y del tamaño adecuado. Cisco ha desarrollado una solución de seguridad específica para las medianas y pequeñas empresas que incorpora los principios de la red de autodefensa.

LA RED DE AUTODEFENSA DE CISCO

La red de autodefensa de Cisco protege las empresas hoy y se adapta a las necesidades futuras. Con Cisco, las empresas pueden proteger no sólo sus redes, sino también su inversión en la red. Como resultado se mejoran los procesos comerciales y se consiguen ahorros substanciales.

Una red de autodefensa de Cisco tiene tres características exclusivas: integración, colaboración y adaptabilidad. En primer lugar, integra la seguridad en todos los elementos de la red, asegurándose de que cada punto de la red pueda defenderse a sí mismo tanto de amenazas internas como externas. En segundo lugar, estos elementos de la red colaboran para intercambiar información a fin de brindar una protección adicional. En tercer lugar, la red utiliza una función innovadora de reconocimiento del comportamiento que permite adaptarse a nuevas amenazas conforme van surgiendo.
Secure Network Foundation de Cisco es una solución de seguridad económica y simplificada, pero a la vez muy completa para las medianas y pequeñas empresas que crea redes de autodefensa confiables.

DESCRIPCIÓN GENERAL DE LA SOLUCIÓN SECURE NETWORK FOUNDATION

La solución Secure Network Foundation de Cisco permite a las medianas y pequeñas empresas enfocar su atención en la rentabilidad, en lugar de en la red. Ofrece servicios seguros y coherentes a todos los usuarios: cableados o inalámbricos. Los servicios de seguridad se integran en los routers, switches y equipos de seguridad de Cisco, ayudando a las medianas y pequeñas empresas a simplificar sus operaciones y reducir costos. La solución Secure Network Foundation de Cisco incorpora la tecnología de red de autodefensa de Cisco que protege a las redes hoy y les permite adaptarse para hacer frente a las necesidades de seguridad en el futuro. Las empresas pueden seguir operando, incluso bajo la amenaza de un ataque, y pueden satisfacer los requisitos legales y de sus clientes con respecto a la privacidad y la seguridad de los datos.

Continuar las operaciones del negocio, aun siendo objeto de un ataque

Con el incremento del número de ataques, las empresas y los clientes necesitan garantías de que están protegidos contra los trastornos y bloqueos de los servicios o la manipulación de sus datos. La red de autodefensa de Cisco, de eficacia comprobada, constituye un enfoque con múltiples facetas que protege a las empresas de los efectos devastadores de gusanos, virus, ataques desde el ciberespacio y de otro tipo.
Los virus y gusanos informáticos y el spyware suelen introducirse en las empresas a través de aplicaciones de IM y correo electrónico, descargas de archivos en la Web o transferencias de archivos, aunque los ataques más sofisticados pueden entrar a través de los servicios inalámbricos móviles o servicios del sistema operativo. Los sistemas de prevención de intrusiones de Cisco (IPS), líderes de la industria, exploran e inspeccionan todo el tráfico entrante en tiempo real, buscando irregularidades que puedan ser indicios de un ataque. Si se detecta una anomalía, un equipo de seguridad de Cisco clasifica la gravedad del riesgo y lo comunica a otros componentes de la red vigilantes de la seguridad. De esta forma, pueden detener la amenaza desde el origen de forma inmediata e impedir que se propague por la red.
Los gusanos, virus y spyware no son la única forma en que son atacadas las empresas. Los equipos de seguridad de Cisco utilizan las mismas funciones de inspección de aplicaciones y del tráfico para detectar y repeler ataques DoS u otros ataques tan nuevos que aún no tienen nombre. La seguridad integrada en toda la empresa detiene los ataques conocidos y desconocidos en tiempo real, y la comunicación entre los componentes de la red les permite adaptarse a los cambios en las condiciones de seguridad. Estas capas de seguridad permiten a las medianas y pequeñas empresas continuar respondiendo a los clientes y mantener sus operaciones comerciales aun cuando están siendo objeto de un ataque

Mantener la privacidad de los clientes

La solución Secure Network Foundation de Cisco utiliza numerosas herramientas para impedir el uso no autorizado de la información de los clientes dentro o fuera de la empresa. Las redes virtuales privadas (VPN) permiten a las pequeñas oficinas y a los trabajadores móviles comunicarse entre sí y con la oficina principal de manera totalmente privada, incluso cuando utilizan Internet para su transporte. Las normas de autenticación de usuarios más avanzadas garantizan que sólo los usuarios válidos puedan acceder a la red VPN. La tecnología sólida de cifrado hace indescifrables los datos para cualquier persona que intente interceptar las comunicaciones de VPN a través de una red pública.
Las funciones de firewall e IPS en cada punto de entrada a la red detienen a los gusanos, spyware o intentos por parte de hackers de penetrar en la red de la empresa para robar información. Los firewalls también son útiles para prevenir que usuarios internos accedan a información de carácter delicado. Por ejemplo, las políticas internas de firewall pueden prevenir el uso por parte de empleados no autorizados de la información financiera, los recursos humanos o las computadoras de contabilidad, o la visualización no autorizada del tráfico de la red. Las redes virtuales LAN (VLAN) permiten a las empresas segmentar aún más sus comunicaciones internas dentro de la organización. La información confidencial de carácter financiero o de los clientes puede guardarse en su propia VLAN, estableciendo una separación lógica con respecto a la red LAN de los empleados.
La solución Secure Network Foundation de Cisco ayuda a las empresas a cumplir los requisitos legales de seguridad y privacidad de la información de sus clientes protegiendo la red contra las violaciones de seguridad o contra los intrusos no autorizados que pretenden acceder desde dentro o fuera de la red.

Controlar costos

La solución Secure Network Foundation de Cisco ayuda a las medianas y pequeñas empresas a controlar sus costos de dos formas: en primer lugar, evitando los costos innecesarios asociados a las infracciones de seguridad; en segundo lugar, haciendo uso de componentes de seguridad integrada económicos y de multifunción que crecen con el negocio a medida que cambian sus necesidades. La seguridad integrada simplifica la administración de la red y los costos de mantenimiento, reduciendo el costo total de propiedad de la red.

Las violaciones en la seguridad de la red conllevan ciertos costos -algunos son evidentes y otros están ocultos-. Por ejemplo, muchas violaciones a la seguridad, por ejemplo virus relativamente inocuos, causan poco daño y los costos evidentes relacionados con ellos son el tiempo y los recursos empleados en eliminarlos de los sistemas empresariales infectados. Los costos se elevan con el número de sistemas infectados, con lo que la protección y la rápida detección requieren un gran esfuerzo para ahorrar costos. Otros costos que no son tan evidentes incluyen la pérdida de tiempo laboral de los empleados durante el período de actualización de los equipos infectados. Algunos ejemplos de costos ocultos incluyen la pérdida de oportunidades, la pérdida de clientes, la disminución de la reputación comercial o los costos legales asociados a las violaciones de seguridad. Estos costos, aunque son menos comunes, pueden ser cuantiosos. El costo para las empresas británicas causado el último año por los delitos cometidos en línea ascendió a 2.400 millones de libras**. La solución Secure Network Foundation de Cisco ayuda a las empresas a evitar tanto los costos evidentes como los ocultos relacionados con las violaciones de seguridad, lo que reduce el riesgo comercial e incrementa la credibilidad del negocio y la confianza de los clientes.

Las medianas y pequeñas empresas no tienen los mismos recursos de personal ni los capitales presupuestarios para desplegar y mantener complejas soluciones de seguridad. La Base para redes seguras de Cisco es segura, confiable y sencilla, y ayuda a reducir el costo total de propiedad de la red, de manera que las organizaciones puedan centrar su atención en sus negocios, no en sus redes. Se adapta fácilmente a los cambios en las necesidades del negocio y de las condiciones de seguridad, garantizando el control de los costos a la par del crecimiento de la empresa.

Construir una base para redes seguras

La solución Secure Network Foundation de Cisco se ha desarrollado basándose en dos familias de productos principales: la familia de routers de servicios integrados de Cisco (ISR) y los dispositivos adaptables de seguridad de la serie Cisco ASA 5500 (ASA). Estas soluciones constituyen los pilares de la red de autodefensa de Cisco para medianas y pequeñas empresas.

Tal y como implica su nombre, los routers de servicios integrados de Cisco (ISR) combinan numerosas funciones en una sola plataforma de routers confiable y accesible adecuada para oficinas de una sola persona u oficinas de mediano o pequeño tamaño. Un ISR de Cisco hace el trabajo de un router de acceso de banda ancha DSL con un enlace redundante integrado, un switch de LAN, punto de acceso inalámbrico y un switch de LAN inalámbrica, todo en un mismo dispositivo. Puesto que es posible añadir estas funciones a los ISR de Cisco según se vayan necesitando, pueden adaptarse con facilidad a los cambios en los requisitos de las medianas y pequeñas empresas. También incorporan muchas funciones de seguridad básicas, que incluyen firewall, IPS y VPN.

El dispositivo adaptable de seguridad de la serie Cisco ASA 5500 es una familia de dispositivos de seguridad integrada de alto rendimiento basada en la tecnología de seguridad demostrada de Cisco que reacciona y se adapta para proteger contra amenazas conocidas y desconocidas. La serie Cisco ASA 5500 combina lo mejor de su clase en firewall, IPS, antivirus de red, inspección de aplicaciones y servicios de VPN de acceso remoto y de sitio a sitio. Un Cisco ASA 5500 proporciona el más elevado nivel de protección contra el acceso por parte de usuarios no autorizados, gusanos, virus, spyware y aplicaciones maliciosas o poco seguras. Este único dispositivo, que integra tecnología de seguridad con eficacia comprobada en el mercado, está diseñado para las redes empresariales de las medianas y pequeñas empresas de hoy en día. Es económico, se despliega y administra fácilmente y es ampliable. A medida que surgen nuevas amenazas contra la seguridad, unas actualizaciones y ampliaciones de seguridad instaladas por el usuario permitirán a los productos ASA de Cisco adaptarse para seguir protegiendo el negocio. La serie Cisco ASA 5500 es la elección perfecta para desplegar en una oficina principal o una sucursal que requiera una protección completa.

Un componente opcional de la solución Secure Network Foundation de Cisco, el switch de la serie Catalyst® Express 500 de Cisco, es una familia de switches inteligentes, sencillos y seguros, diseñados específicamente para las medianas y pequeñas empresas. Todos los switches Catalyst de Cisco contienen funciones de seguridad que detectan irregularidades en el tráfico e impiden que saturen a los switches o se propaguen a otros puntos de la red. Optimizados para las funciones inalámbricas, de datos y voz, el switch Catalyst Express 500 de Cisco ofrece la confiabilidad y seguridad de los switches Catalyst con un factor de forma asequible que se instala en apenas unos minutos. Cada switch Catalyst Express 500 de Cisco se suministra junto con Cisco Network Assistant, una herramienta que configura el switch reconociendo otros componentes de la red.

** Unidad Nacional de Delitos Tecnológicos

Otro componente opcional, los puntos de acceso inalámbrico Cisco Aironet®, ofrecen un acceso seguro a LAN inalámbricas para oficinas de pequeño y mediano tamaño. Los productos inalámbricos de Cisco brindan el mismo nivel de seguridad, escalabilidad y capacidad de administración que una LAN cableada. Los puntos de acceso inalámbrico Cisco Aironet admiten itinerancia o "roaming" rápido y seguro cuando se utilizan con dispositivos de cliente de Cisco o compatibles, lo que permite a los usuarios autenticados desplazarse con seguridad de un punto de acceso a otro.

Combinarlo todo

Un servicio y asistencia excelente y completa es importante para el éxito a largo plazo de cualquier solución de red. Cisco SMB Support Assistant está diseñado para satisfacer las necesidades de las medianas y pequeñas empresas. Es un programa de asistencia técnica económico y fácil de usar que resuelve problemas típicos de las medianas y pequeñas empresas, y garantiza que la red permanezca disponible y segura. Las empresas pueden obtener un diagnóstico a tiempo y consejos para la resolución de problemas junto con reemplazo de piezas por adelantado. Un componente clave del programa es el Portal de Cisco SMB Support Assistant, un conjunto de herramientas seguras en línea que permite a los clientes recuperar contraseñas, acceder a documentación de asistencia, realizar comprobaciones del estado de la red, descargar parches de software y abrir casos de asistencia técnica siempre que sea necesario.

¿POR QUÉ CISCO?

La solución Secure Network Foundation de Cisco para medianas y pequeñas empresas mantiene en funcionamiento los procesos comerciales, asegurándose de que la información de los clientes se mantiene confidencial y que se controlan los costos asociados con el mantenimiento de una red de autodefensa segura y disponible. A cambio, aumenta la confianza de los clientes, se mantiene o aumenta la eficacia de los empleados, se ayuda a las empresas a cumplir los requisitos legales y disminuye el costo total de adquisición.

La solución Secure Network Foundation de Cisco es una de muchas soluciones inteligentes para la mediana y pequeña empresa de Cisco diseñadas para mejorar la eficacia de los empleados, dar apoyo a servicios innovadores, mejorar la satisfacción del cliente y reducir los costos operativos. Con capacidades mejoradas en las áreas de voz, seguridad, movilidad y protección de la inversión, las soluciones de Cisco para medianas y pequeñas empresas satisfacen las necesidades de las empresas hoy y en el futuro.

Cisco y sus partners tienen el compromiso de ofrecer a las medianas y pequeñas empresas la mejor experiencia posible para sus clientes. Opciones de servicio y asistencia de gran prestigio y capacitación personalizada ayudan a las empresas a obtener el máximo beneficio de su solución para medianas y pequeñas empresas por parte de Cisco.

Cisco es líder del mercado en enrutamiento, switching y seguridad, y proporciona soluciones flexibles para satisfacer las necesidades empresariales de hoy y para el futuro, lo que permite a las empresas crecer y operar con agilidad. La estrategia de seguridad de Cisco está basada en la red de autodefensa de Cisco, que integra la seguridad en todos y cada uno de los puntos de la infraestructura, colabora para brindar una protección adicional y se adapta a los cambios en las condiciones de la red y a las nuevas amenazas contra la seguridad.

PASOS A SEGUIR

Para obtener más información sobre la solución Secure Network Foundation de Cisco, póngase en contacto con su partner de Cisco o visite www.cisco.com/global/LA/microsites/snf/espanol/.

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
Parque Empresarial Forum, Edificio C, Segundo Piso
San Jose, Costa Rica.
08000120118 ext 7182653
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
http://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
268 Ave. Munoz Rivera, Hato Rey Tower Suite 2300
Hato Rey, PR 00918
Puerto Rico.
1-800-493-9697 Ext 7182507
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
http://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