

Cisco SA 500 Series Security Appliances

Solución de seguridad "todo en uno" para la protección de empresas en crecimiento

Cisco® SA 500 Series Security Appliances, parte de Cisco Small Business Pro, son soluciones integrales de seguridad para puertas de enlace que combinan firewall y VPN con capacidades opcionales de prevención de intrusiones y servicios de seguridad de correo electrónico y web, lo que garantiza la protección y capacidad de recuperación de su empresa. Estos dispositivos de seguridad de fácil uso le permiten controlar el acceso a los recursos de la red, con el fin de proteger la información de la empresa y maximizar el tiempo de actividad de la red. Los dispositivos Cisco SA 500 Series le ayudan a mejorar la productividad de los empleados al controlar el acceso a Internet, los correos no deseados, los ataques de suplantación de identidad y otras amenazas emergentes y al liberar a los recursos de TI de las actividades relacionadas con la erradicación de virus y la limpieza del sistema. Con los dispositivos Cisco SA 500 Series, puede implementar nuevas aplicaciones empresariales de manera que no se produzcan brechas en el sistema de seguridad. Además, los empleados móviles y los partners de negocios pueden conectarse de manera segura a su red a través de Internet, mediante servicios de red privada virtual con seguridad IP (IPsec) o capa de sockets seguros (SSL). Cuando una solución Cisco SA 500 Series protege su red, puede concentrarse en el crecimiento de su empresa sin preocuparse por las amenazas de seguridad más recientes.

Desafío

Internet se ha convertido en una herramienta comercial crítica para organizaciones de todas las magnitudes, porque ofrece nuevas oportunidades para el crecimiento comercial y permite a los partners y trabajadores remotos tener acceso a la red de una empresa a través de conexiones VPN. Pero, al mismo tiempo, constituye un conducto para introducir amenazas a la red de una empresa que pueden producir impactos negativos de consideración:

- El acceso no autorizado puede provocar la pérdida de datos de la empresa, tiempo de inactividad no planificado y problemas relacionados de responsabilidad legal.
- Los virus pueden infectar los sistemas y provocar interrupciones, lo que resultaría en la pérdida de ingresos.
- El correo electrónico no deseado y la suplantación de identidad crean un gran obstáculo y disminuyen la productividad de los empleados
- El software espía permite obtener un panorama interno de su red e información en forma directa que puede derivar en el robo de identidad o la pérdida de datos de la empresa.
- La navegación por sitios web de carácter nocivo o sin vinculación con el trabajo provoca una merma en la productividad, la exposición a virus y software espía, y posibles problemas de responsabilidad legal que involucren a los empleados.

Solución

Cisco SA 500 Series brinda a las empresas en crecimiento un sistema integral de seguridad para puertas de enlace y conexión de red privada virtual. Al combinar servicios de firewall con seguridad de correo electrónico e Internet, el dispositivo Cisco SA 500 Series detiene las amenazas antes de que ingresen a la red y perjudiquen las operaciones comerciales. Cisco SA 500 Series:

- **Permite el flujo del tráfico válido de la empresa y bloquea los visitantes no deseados:** también admite un área de red de acceso público, conocida como una zona desmilitarizada (DMZ), para hospedar, en forma segura, a servidores web y de archivos, y a otros servidores a los que se puede acceder a través de Internet, sin permitir que la red LAN interna de la empresa quede expuesta a las amenazas.

- **Evita en forma proactiva las intrusiones y bloquea comunicaciones punto a punto peligrosas:** mediante el sistema de prevención de intrusiones (IPS) opcional para la licencia SA 500, el dispositivo SA 500 Series tiene la capacidad de identificar posibles intrusiones a la red de la empresa y actuar para detener la intrusión y evitar riesgos adicionales. Además, el dispositivo SA 500 Series puede bloquear el tráfico punto a punto y la mensajería instantánea, realizar una inspección de protocolo para aumentar la seguridad de la red y la productividad de los empleados, y mantener la red disponible para el tráfico de la información de la empresa.
- **Ofrece protección web total y de correo electrónico a velocidad máxima:** gracias a los potentes recursos de seguridad de contenido, disponibles por suscripción al servicio opcional Cisco ProtectLink Gateway, Cisco SA 500 Series puede ofrecer servicios de seguridad perimetrales cruciales para proporcionar una protección integral:
 - **Protección total a velocidad máxima:** los servicios ProtectLink Gateway se proporcionan a través de un enfoque de nube exclusivo. Los correos electrónicos enviados a su empresa son examinados previamente por Trend Micro, partner tecnológico de Cisco, mediante capacidades de inspección de clase empresarial, con el fin de detener una amplia gama de amenazas. Es decir, el servicio ProtectLink Gateway que examina sus correos electrónicos es capaz de detectar más de 3 millones de patrones de virus y más de 400.000 patrones de software espía. Además, se ofrece protección contra el correo no deseado a través de 10 tecnologías de inspección que no se limitan a evaluar la reputación de la dirección de red del remitente, sino que también controlan el contenido mismo del correo electrónico. Otros productos para empresas en crecimiento no ofrecen un servicio de tales características. Este método no sólo genera beneficios en materia de seguridad, sino que, a diferencia de los sistemas de la competencia, no sacrifica ancho de banda para la inspección de contenido de Internet o correo electrónico y, por ende, no reduce la velocidad del tráfico. Con ProtectLink Gateway, es posible detener una mayor cantidad de amenazas antes de que ingresen a su empresa, sin afectar el ancho de banda.
 - **Antivirus:** una galardonada tecnología antivirus protege los recursos internos de la red contra el ataque de virus conocidos y desconocidos en el punto de su infraestructura donde resulta más eficaz: la puerta de enlace de Internet. Al filtrar el tráfico de Internet y de correo electrónico en el perímetro de la red, se elimina la necesidad de utilizar una gran cantidad de recursos a la limpieza de infecciones, y se garantiza la continuidad de la actividad comercial.
 - **Bloqueo de software espía:** el bloqueo de software espía en la puerta de enlace previene su ingreso a la red mediante el tráfico de Internet (HTTP y FTP) y el correo electrónico, con lo cual se evitan costosos procesos de eliminación y se mejora la productividad de los empleados.
 - **Bloqueo de correo no deseado:** un eficaz bloqueo de los correos no deseados, con un mínimo porcentaje de falsos positivos, ayuda a restaurar la eficacia del correo electrónico, garantizando la continuidad de las comunicaciones con clientes, proveedores y partners.
 - **Bloqueo de la suplantación de identidad:** la protección contra el robo de identidad lo resguarda de ataques de suplantación de identidad, y así se impide que los empleados divulguen involuntariamente datos personales o de la empresa que pudieran ocasionar pérdidas económicas.
 - **Filtrado de URL:** el filtrado de URL y contenido web puede utilizarse para controlar el uso que hacen los empleados de Internet, ya que bloquea el acceso a sitios web inapropiados o sin ninguna relación con el trabajo, lo cual mejora la productividad de los empleados y reduce el riesgo de demandas legales por parte de los empleados a causa de la exposición a contenido ofensivo.
- **Aumenta la seguridad del acceso remoto:** gracias a los servicios de VeriSign Identity Protection (VIP), Cisco SA 500 Series ofrece control de acceso mediante autenticación de dos factores y contraseñas de un solo uso, para aumentar el nivel de seguridad del acceso remoto sin necesidad de adquirir equipos de autenticación adicionales.

- **Es fácil de implementar y administrar:** Cisco SA 500 Series se puede operar a través de la aplicación de configuración integrada Security Appliance Configuration Utility, una potente y sencilla interfaz para administración y supervisión basada en un navegador. Esta solución proporciona una completa gama de funciones de configuración y supervisión en una sola aplicación. La aplicación Security Appliance Configuration Utility también se puede iniciar desde el asistente Cisco Configuration Assistant. Además, Cisco SA 500 Series admite la supervisión del protocolo simple de administración de red (SNMP).

En las Figuras 1 y 2 se muestran las interfaces del asistente Cisco Configuration Assistant y la aplicación Security Appliance Configuration Utility.

Figura 1. Interfaz de Cisco Configuration Assistant

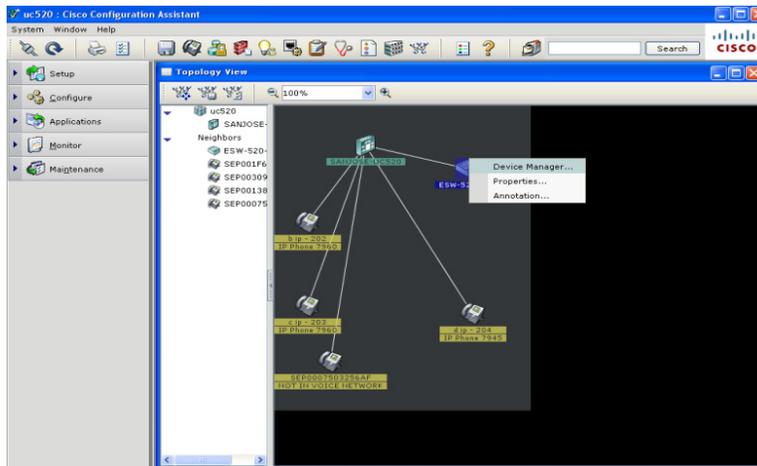
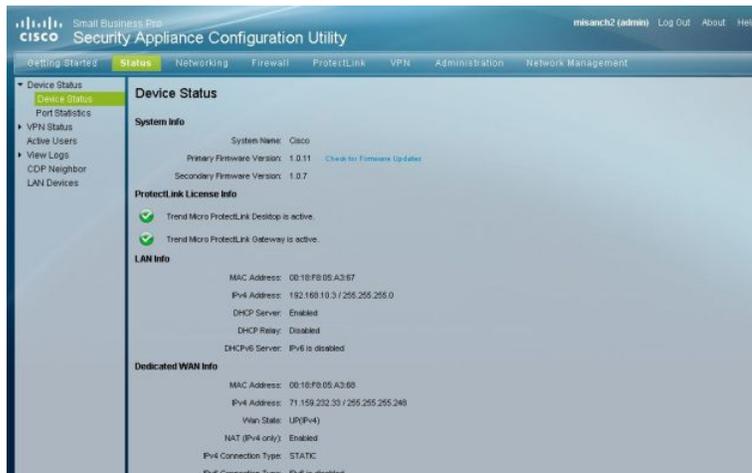


Figura 2. Interfaz de Security Appliance Configuration Utility



Beneficios comerciales

Cisco SA 500 Series Security Appliances garantizan seguridad y conectividad, que le permiten:

- **Acompañar la evolución de las demandas comerciales:** implemente aplicaciones en forma segura. .Proporcione servicios de seguridad de capa de aplicación para la mayoría de las aplicaciones más populares, que incluyen las basadas en la web, correo electrónico, voz sobre IP, video y las aplicaciones multimedia.

- **Mejorar la seguridad en la autenticación para usuarios remotos:** impida el acceso no autorizado a la red de su empresa con contraseñas de un solo uso generadas por hardware o software.
- **Aumentar la productividad de los empleados:** evite la disminución en la productividad de sus empleados con el servicio opcional Cisco ProtectLink Gateway, que le permite bloquear correos electrónicos no deseados y software espía, además de impedir la navegación inapropiada por Internet.
- **Mejorar la capacidad de recuperación de la empresa:** implemente un potente firewall de clase empresarial, junto con capacidades de seguridad de Internet y correo electrónico, para evitar la alteración de servicios y aplicaciones comerciales críticas a causa de violaciones a la seguridad.
- **Reducir costos de TI:** libere recursos de soporte de TI y evite el costoso proceso de eliminación de infecciones causadas por programas espía, virus u otros tipos de software malicioso, al impedir que se produzcan esas infecciones.
- **Proporcionar acceso remoto de fácil implementación:** brinde una conexión de red privada virtual con capa de sockets seguros para que empleados y partners puedan ingresar a la red de la empresa de manera rápida y sencilla.
- **Lograr eficacia operativa:** reduzca los costos asociados con la implementación y con la constante administración y supervisión de la solución de seguridad mediante un producto integrado, de fácil instalación y uso.
- **Reducir las responsabilidades legales:** reduzca la exposición de la empresa a las responsabilidades legales relacionadas con la divulgación de información confidencial o con controles corporativos inadecuados, mediante la implementación de controles de acceso y servicios de protección contra amenazas en un solo dispositivo.
- **Disfrutar de tranquilidad:** obtenga el máximo beneficio de la solución de Cisco mediante un servicio accesible por suscripción. El servicio Cisco Small Business Pro Service contempla actualizaciones de software, acceso integral a Cisco Small Business Support Center y reemplazo de hardware al día hábil siguiente.

Estos beneficios convierten a Cisco SA 500 Series Security Appliance en la opción ideal para satisfacer sus necesidades de seguridad y optimizar el desempeño de la red y los empleados de su empresa.

En la Figura 3 se muestra el dispositivo Cisco SA 500 Series Security Appliance con y sin conexión inalámbrica.

Figura 3. Cisco SA 500 Series Security Appliances: SA 520W y SA 520



Especificaciones del producto

En la Tabla 1 se detallan las especificaciones de los dispositivos de Cisco SA 500 Series.

Tabla 1. Cisco SA 500 Series Security Appliance: modelos y especificaciones

	SA 520	SA 520W	SA 540
Firewall			
Rendimiento de la inspección activa de paquetes*	200 Mbps	200 Mbps	300 Mbps
Rendimiento del firewall más la seguridad de Internet y el correo electrónico*	200 Mbps	200 Mbps	300 Mbps
Conexiones	15.000	15.000	40.000
Reglas	100	100	100
Cronogramas	Sí	Sí	Sí
IPS	Sí	Sí	Sí
Bloqueo de comunicaciones punto a punto y mensajería instantánea	Sí	Sí	Sí
VPN			
Rendimiento de la red privada virtual (VPN) con estándar de triple cifrado de datos (3DES) o estándar de cifrado avanzado (AES)*	65 Mbps	65 Mbps	85 Mbps
Túneles de red privada virtual con IPsec	50 máx.	50 máx.	100 máx.
Túneles de red privada virtual con capa de sockets seguros	2 puestos incluidos; se requiere licencia para ampliar a 25 puestos (máx.)	2 puestos incluidos; se requiere licencia para ampliar a 25 puestos (máx.)	50 puestos (máx.) incluidos
Detección de puntos inactivos	Sí	Sí	Sí
IPsec NAT transversal (NAT-T)	Sí	Sí	Sí
Difusión NetBIOS por VPN	Sí	Sí	Sí
Cisco ProtectLink Gateway			
Filtrado de URL	Más de 80 categorías	Más de 80 categorías	Más de 80 categorías
Protección contra amenazas de la web	Sí	Sí	Sí
Protección contra correo no deseado	Sí	Sí	Sí
Patrones de virus	Más de 3 millones	Más de 3 millones	Más de 3 millones
Patrones de software espía	Más de 420.000	Más de 420.000	Más de 420.000
Tecnología inalámbrica			
802.11b/g/n	No	Sí	No
MIMO (entrada múltiple, salida múltiple) 2 x 3	No	Sí	No
2,4 GHz	No	Sí	No
Calidad de servicio Wi-Fi Multimedia (WMM)	No	Sí	No
Ahorro de energía automático no programado (Ahorro de energía de WMM)	No	Sí	No
Filtrado de MAC	No	Sí	No
Privacidad equiparable a la de redes cableadas (WEP), clave precompartida del protocolo Wi-Fi Protected Access (WPA2-PSK), WPA2-ENT	No	Sí	No
Identificador de conjuntos de servicios básicos o puntos de acceso virtuales	No	Sí; se admiten 4	No
Capacidad de ajustar la potencia de transmisión en forma dinámica o manual	No	Sí	No
Wi-Fi Protected Setup (WPS)	No	Sí	No

Otros			
Enrutamiento	Estático; protocolo de información de enrutamiento (RIP, Routing Information Protocol) v1, v2	Estático; RIP v1, v2	Estático; RIP v1, v2
Redes VLAN	16	16	16
Paso a través de IPsec/protocolo de túneles punto a punto (PPTP)/protocolo de túneles de capa 2 (L2TP)	Sí	Sí	Sí
Resumen de mensaje	MD5/SHA1/SHA2	MD5/SHA1/SHA2	MD5/SHA1/SHA2
Cifrado	DES/3DES/AES	DES/3DES/AES	DES/3DES/AES
Base de datos de usuarios	100	100	400
DNS dinámico	Sí	Sí	Sí
Equilibrio de carga	Sí	Sí	Sí
Integración y automatización de conmutación por fallas y por recuperación	Sí, utilizando el puerto opcional para WAN dual	Sí, utilizando el puerto opcional para WAN dual	Sí, utilizando el puerto opcional para WAN dual
Compatibilidad con VeriSign VIP	Sí	Sí	Sí
Interfaces físicas	<ul style="list-style-type: none"> Todos los puertos Ethernet habilitados para 10BASE-T, 100BASE-TX, 1000BASE-T 4 puertos LAN 1 puerto WAN 1 puerto opcional para usar como puerto LAN, WAN o DMZ 1 puerto USB 2.0 1 switch de alimentación 	<ul style="list-style-type: none"> Todos los puertos Ethernet habilitados para 10BASE-T, 100BASE-TX, 1000BASE-T 4 puertos LAN 1 puerto WAN 1 puerto opcional para usar como puerto LAN, WAN o DMZ 1 puerto USB 2.0 1 switch de alimentación 3 antenas externas 	<ul style="list-style-type: none"> Todos los puertos Ethernet habilitados para 10BASE-T, 100BASE-TX, 1000BASE-T 8 puertos LAN 1 puerto WAN 1 puerto opcional para usar como puerto LAN, WAN o DMZ 1 puerto USB 2.0 1 switch de alimentación
Temperatura ambiente de funcionamiento	De 0 a 40 °C (de 32 a 104 °F)	De 0 a 40 °C (de 32 a 104 °F)	De 0 a 40 °C (de 32 a 104 °F)
Temperatura de almacenamiento	De -20 a 70 °C (de -4 a 158 °F)	De -20 a 70 °C (de -4 a 158 °F)	De -20 a 70 °C (de -4 a 158 °F)
Fuente de alimentación interna			
Rango de voltaje	De 90 a 264 VCA, monofásico	De 90 a 264 VCA, monofásico	De 90 a 264 VCA, monofásico
Frecuencia de entrada	47 a 63 Hz	47 a 63 Hz	47 a 63 Hz
Regulación del voltaje de salida	11,4 V ~ 12,6 V	11,4 V ~ 12,6 V	11,4 V ~ 12,6 V
Corriente de salida	2,5 A máx.	2,5 A máx.	2,5 A máx.
Especificaciones físicas			
Factor de forma	1 RU, 19 pulg. de montaje en bastidor	1 RU, 19 pulg. de montaje en bastidor	1 RU, 19 pulg. de montaje en bastidor
Dimensiones (alto x ancho x profundidad)	1,73 x 12,12 x 7,08 pulg. (44 x 308 x 180 mm)	1,73 x 12,12 x 7,08 pulg. (44 x 308 x 180 mm) sin antenas	1,73 x 12,12 x 7,08 pulg. (44 x 308 x 180 mm)
Peso (con fuente de alimentación interna)	2,23 kg (4,91 lb)	2,34 kg (5,15 lb)	2,34 kg (5,14 lb)

* Metodología de la prueba de rendimiento: el rendimiento máximo está basado en RFC 2544. Todos los resultados corresponden a la suma del rendimiento bidireccional. El rendimiento real puede variar en función del entorno y la configuración de la red.

Pedidos

En la Tabla 2 se enumeran los números de pieza correspondientes a los dispositivos Cisco SA 500 Series Security Appliances.

Tabla 2. Números de pieza de los productos

Producto	SKU
Dispositivo de seguridad SA 520	SA520-K9
Dispositivo de seguridad SA 520W	SA520W-K9
Dispositivo de seguridad SA 540	SA540-K9
ProtectLink Gateway Unlimited Web + 25 puestos de correo electrónico como máximo durante 1 año	L-PL-GW-25MAX-1=
ProtectLink Gateway Unlimited Web + 25 puestos de correo electrónico como máximo durante 3 años	L-PL-GW-25MAX-3=
ProtectLink Gateway Unlimited Web + 100 puestos de correo electrónico como máximo durante 1 año	L-PL-GW-100MAX-1=
ProtectLink Gateway Unlimited Web + 100 puestos de correo electrónico como máximo durante 3 años	L-PL-GW-100MAX-3=
Licencia de IPS para SA 500 Series	L-SA500-IPS-1YR=
Licencia ampliable para 5 puestos de Cisco ProtectLink Endpoint	L-PLEP-5=
Licencia ampliable para 25 puestos de Cisco ProtectLink Endpoint	L-PLEP-25=
Renovación de licencia ampliable para 5 puestos de Cisco ProtectLink Endpoint	L-PLEP-5R=
Renovación de licencia ampliable para 25 puestos de Cisco ProtectLink Endpoint	L-PLEP-25R=
Licencia de SSL para SA 520 y SA 520W	L-FL-SSL-SA520-K9=
Cisco Small Business Pro Service, 3 años	CON-SBS-SVC2
SA 520 con licencias IPS y ProtectLink Web durante 3 años	SA520-WEB-BUN3-K9
SA 520 con 25 licencias IPS y ProtectLink Gateway durante 3 años	SA520-GW25-BUN3-K9
SA 520 con 100 licencias IPS y ProtectLink Gateway durante 3 años	SA520-GW100BUN3-K9
SA 520W con licencias IPS y ProtectLink Web durante 3 años	SA520W-WEB-BUN3-K9
SA 520W con 25 licencias IPS y ProtectLink Gateway durante 3 años	SA520W-GW25BUN3-K9
SA 520W con 100 licencias IPS y ProtectLink Gateway durante 3 años	SA520W-GW100BN3-K9
SA 540 con licencias IPS y ProtectLink Web durante 3 años	SA540-WEB-BUN3-K9
SA 540 con 25 licencias IPS y ProtectLink Gateway durante 3 años	SA540-GW25-BUN3-K9
SA 540 con 100 licencias IPS y ProtectLink Gateway durante 3 años	SA540-GW100BUN3-K9

Conectividad segura para su empresa

La red se está transformando en un componente clave de las operaciones comerciales más importantes. Para que la empresa funcione siempre a la perfección y los clientes reciban un servicio acorde a sus expectativas, debe contar con una red segura, potente y flexible. Los dispositivos Cisco SA 500 Series Security Appliances simplifican las comunicaciones, ya que permiten conectar a los clientes con la empresa y a los empleados entre sí. Los dispositivos proporcionan las potentes funciones de protección, acceso seguro a la red privada virtual y enrutamiento avanzado que usted necesita. Al mismo tiempo, le ayudan a controlar los costos, reducir la necesidad de incorporar equipos separados y simplificar la administración de la red. Si está poniendo en marcha una nueva empresa o está expandiendo una empresa ya exitosa, los dispositivos Cisco SA 500 Series Security Appliances pueden ayudarle a mantenerse conectado y a crecer sin inconvenientes en el futuro.

Servicio y soporte técnico

Los dispositivos Cisco SA 500 Series Security Appliances cuentan con el respaldo del servicio Cisco Small Business Pro Service, cuya cobertura accesible le garantiza total tranquilidad. Este servicio por suscripción le permite obtener el máximo beneficio de la serie de productos Cisco Small Business Pro. Provisto por Cisco, este servicio integral incluye actualizaciones y mejoras de software, acceso extendido a Cisco Small Business Support Center y reemplazo de hardware el día hábil siguiente (cuando resulte necesario). El soporte técnico está basado en los conocimientos de la comunidad, de manera que las empresas en crecimiento puedan colaborar e intercambiar conocimientos por medio de wikis y foros en línea para contribuir a la mejora de la eficacia comercial, la identificación y reducción de riesgos, y la atención al cliente.

Más información

Si desea obtener más información sobre Cisco SA 500 Series Security Appliances, visite <http://www.cisco.com/go/sa500> o comuníquese con su proveedor local de Cisco.

Para obtener más información sobre los productos Cisco ProtectLink Gateway y Endpoint, visite <http://www.cisco.com/go/protectlink> o comuníquese con su proveedor local de Cisco.

Si desea obtener más información sobre el producto VeriSign VIP, visite <http://www.cisco.com/go/viptoken> o comuníquese con su proveedor local de Cisco.

Para obtener más información sobre Cisco Small Business Pro Service, visite <http://www.cisco.com/go/proservice>.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)