



Os cinco principais problemas de segurança das PME

RESUMO

As pequenas e médias empresas utilizam a Internet e aplicações em rede para chegar a novos clientes e servir mais eficazmente os clientes já existentes. Por outro lado, novas ameaças à segurança e novas legislações aumentam a pressão sobre as redes empresariais, para que sejam fiáveis e seguras. A Cisco Systems fornece soluções de segurança integradas, abrangentes e acessíveis, adaptadas às necessidades de pequenas e médias empresas. Estas soluções ajudam a garantir a continuidade da actividade empresarial, manter a privacidade dos clientes e reduzir custos operacionais. As empresas podem despendar tranquilamente mais tempo a fomentar as suas actividades empresariais e perder menos tempo com problemas de segurança de rede.

DESAFIOS EMPRESARIAIS

No competitivo mercado global de hoje, as pequenas e médias empresas têm de estar concentradas na expansão das respectivas organizações e no aumento da satisfação dos clientes, sem esquecer o controlo dos custos. Felizmente, a Internet e as aplicações em rede criaram um ambiente competitivo mais equilibrado. As pequenas e médias empresas utilizam as respectivas redes para expandir o alcance de mercado e comunicar com os clientes e parceiros de forma rápida e económica. Contudo, embora permita uma actividade de e-business rápida e ágil, o acesso também pode deixar a empresa exposta a dispendiosas quebras de segurança. É mais importante que nunca ter uma rede fiável, segura e disponível. É igualmente importante que a rede seja flexível e escalável, de forma a acomodar futuras necessidades de largura de banda e serviços avançados, tais como aplicações sem fios e aplicações de voz e dados convergentes.

PROBLEMAS DE SEGURANÇA

De acordo com estudos recentes, a segurança é o maior desafio que as pequenas e médias empresas enfrentam. As ameaças de segurança em contínua mudança, tanto provenientes do interior como do exterior da rede empresarial, podem prejudicar gravemente as actividades empresariais, afectando a rentabilidade da empresa e a satisfação do cliente. Além disso, as pequenas e médias empresas têm de actuar em conformidade com novos regulamentos e leis criados para proteger a privacidade dos consumidores e as informações electrónicas.

Problema de segurança n.º 1: *Worms* e vírus

Os *worms* e vírus informáticos permanecem a ameaça de segurança mais comum, sendo que 75 por cento das pequenas e médias empresas foram afectadas por pelo menos um vírus no último ano¹. Os *worms* e vírus podem ter um efeito devastador na continuidade e rentabilidade da actividade empresarial. Estirpes mais inteligentes e destrutivas estão a disseminar-se mais rapidamente do que nunca, infectando escritórios inteiros em segundos. A limpeza dos computadores infectados é mais demorada, sendo que o processo resulta frequentemente em encomendas perdidas, bases de dados danificadas e clientes irritados. Enquanto as empresas se debatem por actualizar os seus computadores com os mais recentes *patches* de sistema operativo e programas de software antivírus, novos vírus podem furar estas defesas em qualquer momento. Por outro lado, os empregados disseminam vírus e *spyware* quando acedem inadvertidamente a websites maliciosos, transferem material inseguro e indesejado ou abrem anexos de correio electrónico. Embora estes ataques sejam atraídos involuntariamente para a empresa, os mesmos podem provocar significativas perdas financeiras. Os sistemas de segurança têm de detectar e afastar *worms*, vírus e *spyware* em todos os pontos da rede.

¹ Maritz Research, 2005

Problema de segurança n.º 2: Roubo de informações

O roubo de informações é lucrativo. Piratas informáticos penetram em redes empresariais para roubar números de cartões de crédito ou de segurança social para proveito próprio. As pequenas e médias empresas são encaradas como um alvo mais fácil do que as grandes empresas. A protecção do perímetro da rede é um bom começo, mas não é suficiente, pois muitos roubos de informação são auxiliados por uma pessoa infiltrada de confiança (por exemplo, um empregado ou subcontratado).

O roubo de informações pode ter um elevado preço para pequenas e médias empresas, pois o crescimento da actividade empresarial está dependente de clientes satisfeitos e de uma boa reputação. As empresas que não protejam adequadamente as informações poderão deparar-se com publicidade negativa, coimas ou até mesmo processos judiciais. Por exemplo, na Califórnia, entraram em vigor novas leis de protecção do consumidor que exigem que as empresas notifiquem todos os clientes se houver suspeitas de que informações de consumidores foram visualizadas por pessoas não autorizadas. Qualquer estratégia de segurança tem de evitar o roubo de informações electrónicas sensíveis, tanto a partir do interior como do exterior da empresa.

Problema de segurança n.º 3: Disponibilidade dos serviços

Os *worms* e vírus informáticos não são a única ameaça à disponibilidade dos serviços das empresas. Ataques do tipo *denial-of-service* podem encerrar websites e operações de comércio electrónico recorrendo ao envio de grandes volumes de tráfego para um elemento de rede crítico, fazendo com que este falhe ou não consiga processar tráfego legítimo. Mais uma vez, os resultados são desastrosos: perda de dados e encomendas, e pedidos de clientes sem resposta. Se estes ataques forem tornados públicos, a credibilidade da empresa é prejudicada. Embora a maior parte da atenção em torno da indisponibilidade por ataques *denial-of-service* esteja concentrada em grandes instituições bancárias e empresas da lista Global 500, as pequenas e médias empresas não estão imunes. São encaradas como estando menos preparadas para ataques do que as grandes empresas.

Muitos ataques menos dramáticos, mas mais comuns, também ameaçam a disponibilidade dos serviços. Por exemplo, um ataque de roubo de recursos abre brechas em redes e computadores empresariais, utilizando-os para a partilha ilegal de ficheiros de música, filmes ou software. Muitas vezes, as empresas não têm conhecimento da existência de uma brecha na segurança. Enquanto isso, os respectivos computadores e redes respondem lentamente aos clientes, sendo que a participação involuntária das empresas na partilha ilegal de ficheiros as deixa vulneráveis a processos judiciais.

Problema de segurança n.º 4: O desconhecido

A par de cada avanço na área da informática e das comunicações surgem novas formas de explorar essa tecnologia para obter proveito próprio ou prejudicar terceiros. Essas oportunidades são potenciadas pelo lançamento de novo hardware ou software. Por exemplo, quando as aplicações peer-to-peer e de mensagens instantâneas ainda eram relativamente recentes, os utilizadores eram atacados por código malicioso escrito especificamente para essas aplicações. Agora, os telemóveis são alvos frequentes de vírus. Sem a capacidade de prever o que virá a seguir, a melhor defesa é aquela que se consiga adaptar facilmente a futuras ameaças e que seja financeiramente acessível.

Problema de segurança n.º 5: Legislação de segurança

Além destas ameaças à segurança, novos regulamentos e leis obrigam as pequenas e médias empresas a proteger a privacidade e integridade das informações que lhes são confiadas. Na União Europeia, por exemplo, a Directiva de Protecção de Dados regula a protecção de dados pessoais ao cuidado de organizações. Praticamente todos os sectores de actividade têm um exemplo de legislação que regula as actividades empresariais e requer medidas de segurança adicionais. Nos Estados Unidos, a Lei de Portabilidade e Responsabilidade de Sistemas de Saúde (HIPAA, *Health Insurance Portability and Accountability Act*) requer que as organizações de cuidados de saúde, incluindo todos os consultórios médicos, implementem medidas de segurança para garantir a privacidade das informações de saúde e impedir o acesso não autorizado.

Cabe às empresas a obrigação de actuar em conformidade com as leis e os regulamentos aplicáveis à respectiva actividade empresarial no mercado. Os clientes querem garantia de confidencialidade das respectivas informações. Todas as empresas têm de tomar medidas para proteger a infra-estrutura empresarial. Contudo, com os seus orçamentos limitados, as pequenas e médias empresas, em particular, necessitam de soluções simples, adequadas à sua dimensão e financeiramente acessíveis.

CISCO SMART BUSINESS ROADMAP

O Smart Business Roadmap da Cisco permite que as pequenas e médias empresas alinhem os planos tecnológicos com as prioridades da actividade empresarial. Fornece uma evolução estruturada para ajudar as empresas a acompanharem proactivamente as mudanças. Além disso, oferece às empresas e aos decisores técnicos a confiança de saberem que os investimentos imediatos em tecnologia irão suportar os objectivos de longo prazo.

Para orientar as empresas em crescimento ao longo de cada etapa de desenvolvimento (implementação, crescimento e optimização), o Cisco Smart Business Roadmap oferece uma abordagem em duas fases:

- A Rede de Autodefesa (Self-Defending Network) da Cisco
- A Arquitectura de Rede Segura (Secure Network Foundation) da Cisco

A Rede de Autodefesa da Cisco (Self-Defending Network)

A Rede de Autodefesa da Cisco consiste numa estratégia a longo prazo para proteger os processos empresariais através da identificação, prevenção e adaptação a ameaças internas e externas. A Rede de Autodefesa da Cisco protege as empresas no presente e adapta-se a futuras necessidades. Com a Cisco, as empresas podem proteger não só as suas redes, mas também os seus investimentos. Os resultados são processos empresariais melhorados e poupanças substanciais.

Uma Rede de Autodefesa da Cisco tem três características únicas: integração, colaboração e adaptabilidade. Em primeiro lugar, integra a segurança em todos os elementos na rede, garantindo que cada ponto na rede se consegue defender a si próprio de ameaças internas e externas. Em segundo lugar, estes elementos de rede trabalham em conjunto para trocar informações e fornecer protecção adicional. Em terceiro lugar, a rede utiliza um reconhecimento inovador de comportamentos para se adaptar a novas ameaças à medida que estas vão surgindo. A Rede de Autodefesa da Cisco é uma solução de segurança económica e simplificada, mas abrangente, para pequenas e médias empresas, criando redes seguras e com autodefesa.

A Arquitectura de Rede Segura da Cisco (Secure Network Foundation)

A Arquitectura de Rede Segura da Cisco baseia-se numa estrutura de Rede de Autodefesa. Permite que as pequenas e médias empresas se concentrem na rentabilidade e não na rede. Fornece serviços consistentes e seguros a todos os utilizadores, através de redes com ou sem fios. Os routers, switches e dispositivos de segurança da Cisco dispõem de serviços de segurança integrados, ajudando as pequenas e médias empresas a simplificar as operações e a reduzir os custos. A Arquitectura de Rede Segura da Cisco incorpora a tecnologia de Rede de Autodefesa da Cisco, a qual protege a rede no presente e se adapta para enfrentar as necessidades de segurança futuras. As empresas podem continuar a operar, mesmo quando sujeitas a ameaças, e satisfazer os pedidos dos clientes e os requisitos legais em termos de segurança e privacidade dos dados.

Mantenha-se operacional, mesmo sob ataque

Com o crescimento dos ataques, as empresas e os clientes necessitam de ter a garantia de que estão protegidos contra interrupções e custos associados à indisponibilidade do serviço ou dados danificados. A Rede de Autodefesa da Cisco é uma abordagem comprovada e multifacetada que protege as empresas contra os efeitos devastadores de *worms*, vírus, “ciberterrorismo” e outros ataques.

Normalmente, os vírus, *worms* e *spyware* introduzem-se numa empresa por correio electrónico ou aplicações de mensagens instantâneas, por transferências Web ou por transferências de ficheiros, embora possam ocorrer ataques sofisticados por meio de serviços móveis sem fios ou serviços de sistema operativo. Os sistemas de prevenção de intrusão (IPS, Intrusion Prevention Systems) da Cisco são líderes de mercado –

disponíveis nos switches, routers e dispositivos de segurança da Cisco – e analisam e inspecionam em tempo real todo o tráfego de entrada, procurando anomalias que possam denunciar um ataque. Se for detectada uma anomalia, o IPS classifica a gravidade do risco e comunica com outros componentes de rede com suporte de segurança, no sentido de deter a ameaça na origem e impedir que a mesma se propague pela rede.

Uma segurança integrada em toda a empresa bloqueia ataques conhecidos ou desconhecidos em tempo real, sendo que a comunicação entre componentes de rede permite uma adaptação a condições de segurança em mudança. Estas camadas de segurança permitem que pequenas e médias empresas continuem a responder aos clientes e se mantenham operacionais, mesmo sob ataque.

Manter a privacidade dos clientes

Uma Arquitectura de Rede Segura da Cisco utiliza muitas ferramentas para manter as informações dos clientes a salvo de utilizadores não autorizados dentro ou fora da empresa.

Redes privadas virtuais (VPN, Virtual Private Networks) com protocolo IPSec (IP Security) e protocolo SSL (Secure Socket Layer) permitem que pequenos escritórios e trabalhadores remotos comuniquem entre si e com a filial em total privacidade, mesmo ao utilizar a Internet pública para transporte. Os mais seguros padrões de autenticação de utilizador garantem que apenas utilizadores autorizados podem aceder à VPN. Tecnologias de encriptação forte tornam os dados ininteligíveis para qualquer pessoa que tente interceptar as comunicações de VPN numa rede pública. A segurança *endpoint* do Cisco Secure Desktop procura minimizar a quantidade de dados (tais como *cookies*, histórico do *browser*, ficheiros temporários e conteúdo transferido) que fica para trás depois de terminada uma sessão de VPN com SSL.

As capacidades de firewall e IPS em cada ponto de entrada na rede ajudam a bloquear *worms*, *spyware* ou tentativas de penetração na rede empresarial por parte de piratas informáticos para roubo de informações. Os firewalls também são úteis para evitar que utilizadores internos acessem a informações sensíveis. Por exemplo, políticas internas de firewall podem impedir que empregados não autorizados acessem a computadores do departamento financeiro, de recursos humanos ou de contabilidade, ou que visualizem o respectivo tráfego. Redes locais virtuais (VLAN, Virtual Local Area Network) permitem que as empresas segmentem ainda mais as comunicações internas nas respectivas organizações. Informações financeiras ou de cliente sensíveis podem ser colocadas numa VLAN própria, logicamente independente das LAN dos empregados. A Arquitectura de Rede Segura da Cisco ajuda as empresas a cumprir requisitos legais de segurança e de privacidade das informações de clientes, protegendo a rede contra brechas na segurança ou contra intrusos provenientes de dentro ou fora da rede.

Controlo de custos

A Arquitectura de Rede Segura da Cisco ajuda as pequenas e médias empresas a controlar de duas formas os custos: em primeiro lugar, evitando os custos desnecessários associados a brechas na segurança; em segundo lugar, utilizando componentes de segurança integrados multifuncionais e a custo acessível que acompanham o crescimento das empresas à medida que as necessidades se alteram. A segurança integrada simplifica a gestão de rede e os custos de manutenção, reduzindo o custo total de propriedade da rede.

Brechas na segurança da rede têm custos óbvios e ocultos. Por exemplo, muitas falhas de segurança (tais como vírus relativamente inócuos) causam poucos danos, sendo que os custos óbvios associados são o tempo e os recursos despendidos na recuperação dos sistemas empresariais infectados. O aumento dos custos é proporcional ao número de sistemas infectados, fazendo com que a protecção e uma rápida detecção sejam um esforço economizador. Custos menos óbvios incluem o tempo de trabalho perdido durante a recuperação dos computadores infectados dos empregados. Exemplos de custos ocultos incluem oportunidades perdidas, clientes perdidos, reputação empresarial afectada ou custos legais associados a brechas na segurança. Embora menos comuns, estes custos podem ser substanciais. Em 2005, o crime online custou 2,4 mil milhões de libras² às empresas britânicas. A solução Arquitectura de Rede Segura da Cisco ajuda as empresas a evitar os custos óbvios e os custos ocultos associados a brechas na segurança, reduzindo o risco da actividade empresarial e aumentando a credibilidade da empresa e a confiança dos clientes.

² National Hi-Tech Crime Unit (unidade britânica de combate aos crimes de alta tecnologia)

As pequenas e médias empresas não têm os recursos humanos nem os orçamentos necessários para implementar e manter soluções de segurança complexas. A Arquitectura de Rede Segura da Cisco é segura, fiável e simples, ajudando as empresas a reduzir o custo total de propriedade da rede, para que se possam concentrar na respectiva actividade empresarial, e não nas redes. A Arquitectura de Rede Segura adapta-se facilmente às necessidades empresariais e às condições de segurança em mudança, garantindo que os custos são adequados ao crescimento da empresa.

CRIAR UMA ARQUITECTURA DE REDE SEGURA

A Arquitectura de Rede Segura da Cisco inclui vários produtos da Cisco:

- Routers com serviços integrados da Cisco
- Dispositivos de segurança adaptáveis da série ASA 5500 da Cisco
- Switches Catalyst da Cisco
- Pontos de acesso Aironet da Cisco

Estes produtos fornecem os pilares da Rede de Autodefesa da Cisco para pequenas e médias empresas.

Routers com serviços integrados da Cisco

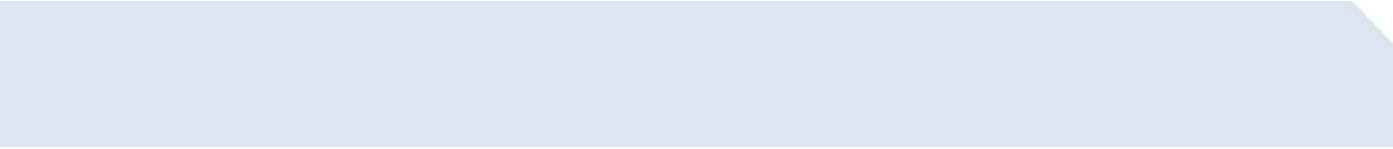
Os routers com serviços integrados da Cisco combinam muitas funcionalidades numa plataforma de router única, fiável e financeiramente acessível. Um router com serviços integrados da Cisco combina as capacidades de um router de acesso de banda larga de cabo ou DSL com uma ligação redundante integrada, um switch de LAN, uma firewall de IPS ou VPN, um ponto de acesso sem fios e um switch de LAN sem fios, tudo num único dispositivo. Muitas destas capacidades podem ser adicionadas a routers com serviços integrados da Cisco consoante necessário, para que as empresas as possam adicionar à medida que as suas necessidades evoluem. Adequados para escritórios unipessoais ou escritórios de pequena ou média dimensão, estes dispositivos disponibilizam uma arquitectura inteligente para futuras necessidades de rede. Quando necessário, as empresas podem adicionar serviços de segurança, de rede sem fios e de dados e voz, sem necessidade de investimentos adicionais financeiros em equipamento.

Dispositivos de segurança adaptáveis da série ASA 5500 da Cisco

A série ASA 5500, de dispositivos de segurança adaptáveis e de alto desempenho, baseia-se na comprovada tecnologia de segurança da Cisco que reage e se adapta para disponibilizar protecção contra ameaças conhecidas e desconhecidas. A série ASA 5500 da Cisco combina os seguintes elementos de topo de gama: firewall; IPS; protecção anti-X contra vírus, *spam* e *spyware*; e serviços VPN de acesso remoto e de peer-to-peer. A série ASA 5500 da Cisco fornece o mais elevado nível de protecção contra acesso de utilizadores não autorizados, *worms*, vírus, *spyware* e aplicações suspeitas ou maliciosas. Este dispositivo único foi concebido para as redes das pequenas e médias empresas de hoje. É económico, de fácil implementação e gestão, e actualizável. À medida que surgem novas ameaças à segurança das redes, actualizações e extensões de segurança instaladas pelo utilizador irão permitir que os produtos ASA da Cisco se adaptem para continuar a proteger as empresas. A série ASA 5500 da Cisco é a escolha perfeita para implementação numa sede ou numa filial que requeira segurança abrangente.

Switches Catalyst da Cisco

Os switches Catalyst da Cisco dispõem das funcionalidades necessárias para proporcionar redes inteligentes, simples e seguras. Foram concebidos para satisfazer exigentes requisitos de segurança, desempenho e fiabilidade. Dado que permitem a convergência de aplicações numa rede, os switches Catalyst da Cisco melhoram a capacidade de resposta dos empregados aos clientes, aumentando também significativamente a eficácia operacional. Todos os switches Catalyst da Cisco contêm funcionalidades de segurança que detectam irregularidades de tráfego e as impedem de sobrecarregar o switch ou chegar a outros pontos na rede.



O Cisco Network Assistant consiste num conjunto gratuito de ferramentas de gestão de fácil utilização para simplificar a instalação, configuração, gestão de rede e resolução de problemas em determinados switches Catalyst da Cisco. O Smartports Advisor consiste numa ferramenta inteligente de configuração que detecta automaticamente todos os dispositivos ligados da Cisco e recomenda configurações predefinidas para a porta de switch ligada ao dispositivo em questão. Simplifica a entrada em funcionamento das redes, permitindo às empresas concentrarem-se em implementações tecnológicas avançadas. A ferramenta Troubleshooting Advisor identifica automaticamente potenciais problemas de rede, tais como problemas de cablagem e erros de configuração, registando-os num gráfico apropriado. Fornece também descrições de problemas e permite que os utilizadores tomem medidas correctivas com um único clique.

Pontos de acesso Aironet da Cisco

Os pontos de acesso Aironet da Cisco fornecem acesso seguro de LAN sem fios para escritórios de pequena e média dimensão. Os produtos sem fios da Cisco expandem o mesmo nível de segurança, escalabilidade e capacidade de gestão de uma LAN com fios. Os pontos de acesso Aironet da Cisco suportam itinerância rápida e segura quando utilizados com dispositivos cliente da Cisco ou compatíveis, permitindo que utilizadores autenticados se desloquem de forma segura entre pontos de acesso.

Funcionamento estável e fiável

Um funcionamento e suporte de excelência e abrangentes são importantes para o êxito a longo prazo de qualquer solução de rede. O Cisco SMB Support Assistant foi concebido para satisfazer as necessidades de pequenas e médias empresas. É um programa auxiliar económico e de fácil utilização que resolve os problemas com que as pequenas e médias empresas normalmente se deparam, garantido que a rede permanece disponível e segura. As empresas podem obter sugestões atempadas de diagnóstico e de resolução de problemas, acelerando-se assim a substituição de componentes. O Cisco SMB Support Assistant Portal consiste num portfólio seguro de ferramentas online que permite que os clientes recuperem senhas, acedam a documentação de suporte, efectuem verificações ao estado de funcionamento da rede, transfiram *patches* de software e efectuem pedidos de suporte técnico quando necessário.

PORQUÊ A CISCO?

A Arquitectura de Rede Segura da Cisco para pequenas e médias empresas mantém os processos empresariais em funcionamento, certifica-se de que as informações de clientes permanecem privadas e controla os custos associados à manutenção de uma rede segura e disponível com autodefesa. Por sua vez, aumenta a confiança dos clientes, mantém ou aumenta a eficácia dos empregados, ajuda as empresas a cumprir requisitos legais e reduz o custo total de propriedade da rede.

A Arquitectura de Rede Segura da Cisco faz parte de uma série de soluções inteligentes do Cisco Smart Business Roadmap da Cisco concebidas para melhorar a eficácia dos empregados, suportar serviços inovadores, melhorar a satisfação dos clientes e reduzir custos operacionais. Com capacidades avançadas nas áreas de voz, segurança, mobilidade e protecção de investimentos, as soluções do Cisco Smart Business Roadmap conseguem satisfazer as necessidades das empresas no presente e no futuro.

A Cisco e os seus parceiros de canal estão empenhados em oferecer a melhor experiência de cliente possível às pequenas e médias empresas. Opções de financiamento, suporte, serviços e formação personalizada ajudam as empresas a tirar o máximo proveito da solução Cisco Smart Business Roadmap.

A Cisco é líder do mercado de routers, switches e segurança, fornecendo soluções flexíveis para satisfazer as necessidades das empresas no presente e no futuro, permitindo-lhes crescimento e agilidade. A estratégia de segurança da empresa baseia-se na Rede de Autodefesa da Cisco, a qual integra a segurança em todos os pontos da infra-estrutura, actua em colaboração para fornecer protecção adicional e se adapta a condições de rede em mudança e nova ameaças de segurança. A Cisco oferece um vasto portfólio de produtos e o Smart Business Roadmap para ajudar pequenas e médias empresas a desenhar um caminho de crescimento inteligente e estruturado, de modo a tirarem o máximo partido dos seus investimentos em tecnologia.



PRÓXIMOS PASSOS

Para mais informações sobre a Arquitectura de Rede Segura da Cisco, contacte o seu parceiro Cisco ou visite: http://www.cisco.com/en/US/netsol/ns644/networking_solutions_packages_list.html.

Para mais informações sobre o Cisco Smart Business Roadmap, contacte o seu parceiro Cisco ou visite: <http://www.cisco.com/go/sbr>.

Para localizar um parceiro de canal da Cisco, visite: <http://www.cisco.com/go/partnerlocator>.

Para mais informações sobre como financiar a sua Arquitectura Segura de Rede, visite: <http://www.cisco.com/go/ciscocapital>.



Escritório Portugal
Cisco Systems Portugal
Quinta da Fonte
Ed. Gil Eanes, A – 1º
2770-192 Paço de Arcos
Portugal
www.cisco.pt
Tel: +351 21 446 8700
Fax: +351 21 446 8701

Sede Corporativa
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
EUA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100


Sede Europa
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
Holanda
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Sede Américas
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
EUA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Sede Ásia-Pacífico
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

A Cisco Systems tem mais de 200 escritórios nos seguintes países e regiões. Pode encontrar todas as Moradas, Números de Telefone e Fax no **Website Cisco.com em www.cisco.com/go/offices.**

Argentina • Austrália • Áustria • Bélgica • Brasil • Bulgária • Canadá • Chile • China • Colômbia • Costa Rica • Croácia • Chipre
República Checa • Dinamarca • Dubai, EAU • Finlândia • França • Alemanha • Grécia • Hong Kong • Hungria • Índia • Indonésia
Irlanda • Israel • Itália • Japão • Coreia • Luxemburgo • Malásia • México • Holanda • Nova Zelândia • Noruega • Peru • Filipinas
Polónia • Portugal • Porto Rico • Roménia • Rússia Arábia Saudita • Escócia • Singapura • Eslováquia • Eslovénia • África do Sul
Espanha • Suécia • Suíça • Taiwan • Tailândia • Turquia • Ucrânia • Reino Unido • Estados Unidos • Venezuela • Vietname • Zimbabué

 Copyright ? 2005 Cisco Systems, Inc. Todos os direitos reservados. CCIP, CCSP, a marca Cisco Powered Network, Cisco Unity, Follow Me Browsing, FormShare e StackWise são marcas comerciais da Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn e iQuick Study são marcas de serviço da Cisco Systems, Inc.; e Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, o logótipo Cisco Certified Internetwork Expert, Cisco IOS, o logótipo Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, o logótipo Cisco Systems, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, o logótipo iQ, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, MICA, o logótipo Networkers, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stram, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath e VCO são marcas comerciais registadas da Cisco Systems, Inc. e/ou respectivas empresas afiliadas nos Estados Unidos e determinados outros países.

As restantes marcas comerciais mencionadas neste documento ou no Website pertencem aos respectivos proprietários. A utilização da palavra parceiro não implica relação de parceria entre a Cisco e qualquer outra empresa. (0501R)