



Estratégia McAfee Protection-in-Depth

Criando Soluções de Segurança Econômicas para Empresas de Pequeno e Médio Porte

Índice

Resumo	3
De onde surgem os riscos à segurança?	3
Protegendo sua rede — opiniões do mercado	3
A Network Associates pode ajudar você a aumentar a segurança de sua rede	4
Soluções McAfee System Protection para empresas de pequeno e médio porte	4
McAfee System Protection—Active Virus Defense Small Business Edition	4
McAfee System Protection—VirusScan ASaP	4
McAfee System Protection—McAfee SpamKiller for Microsoft Exchange	5
Soluções McAfee Network Protection empresas de pequeno e médio porte	5
McAfee Network Protection—McAfee IntruShield 1200	5
McAfee Network Protection—Netasyst Network Analyzer Distributed	5
McAfee Network Protection—Netasyst Network Analyzer LAN	5
McAfee Network Protection—Netasyst Network Analyzer Wireless	5
McAfee Network Protection—Sniffer Portable	5
McAfee Network Protection—Sniffer Reporter	5
Conclusão	6

Resumo

O fato de ter uma empresa de pequeno ou médio porte (SMB) não significa que você não tenha as mesmas necessidades de segurança de rede das grandes empresas. Com funcionários e contratados trabalhando para você em escritórios domésticos, conectando-se à sua rede em localidades remotas ou acessando materiais em quartos de hotel, a necessidade de oferecer segurança ininterrupta é cada vez maior.

Infelizmente, ao implementar todas as tecnologias e proteções de acesso remoto, a única diferença entre as grandes empresas e as SMBs é a quantidade de dinheiro e recursos.

Neste trabalho, discutiremos o seguinte: como a segurança das redes pode ser violada; criação de uma rede segura, bem como ferramentas reconhecidas pelo mercado e, finalmente, mostraremos como a Network Associates® tem as soluções ideais que se adaptam às necessidades de segurança de sua rede.

De onde surgem os riscos à segurança?

Com muita frequência, o patrimônio de muitas empresas está nos sistemas de computador, os quais exigem proteção especializada. Por isso a primeira preocupação do gerente de TI é solucionar de maneira rápida e fácil os problemas de rede e segurança. A chave para a resolução de problemas de segurança é compreender de onde surgem as ameaças. Vejamos algumas formas pelas quais a segurança pode ser violada.

Uma das primeiras coisas a fazer é compreender que tipo de rede existe no momento. Por exemplo, independentemente do nível geral de segurança de sua rede, as LANs sem fio podem ser o alvo preferido, pois exigem pouca invasão física e, muitas vezes, impõem muito menos barreiras de segurança a ser transpostas do que em um ataque pela Internet.

Além disso, sua empresa pode ser gravemente colocada fora de operação devido a uma infecção por vírus e worms, que levará à degradação do desempenho de sua rede ou até mesmo a danos físicos por meio da corrupção ou exclusão de arquivos. Mas nem todas as violações de segurança vêm de fora. Funcionários descontentes, servidores defeituosos, falhas de hardware ou simples acidentes também podem comprometer a segurança internamente.

Protegendo sua rede – opiniões do mercado

A melhor defesa contra ataques externos é reforçar a proteção de sua rede e de seus usuários. Essa medida reduzirá o número de pontos de entrada vulneráveis para que você possa tomar a iniciativa de monitorá-los e implementar medidas antiinvasão, tais como varredura de vírus, prevenção contra invasões, filtragem de spam e firewalls.

Saber o que acontece em sua rede 24 horas por dia — e não apenas nos horários de pico ou durante o horário comercial — ajuda a fortalecer essa proteção. Com o monitoramento

dos padrões de tráfego e de uso, é possível identificar quem está na rede e quais informações estão sendo acessadas. Ao estabelecer um parâmetro básico da atividade de sua rede, você pode detectar padrões incomuns de tráfego que indiquem uma violação de segurança, a maneira como a violação ocorreu e o que pode ser feito para solucioná-la.

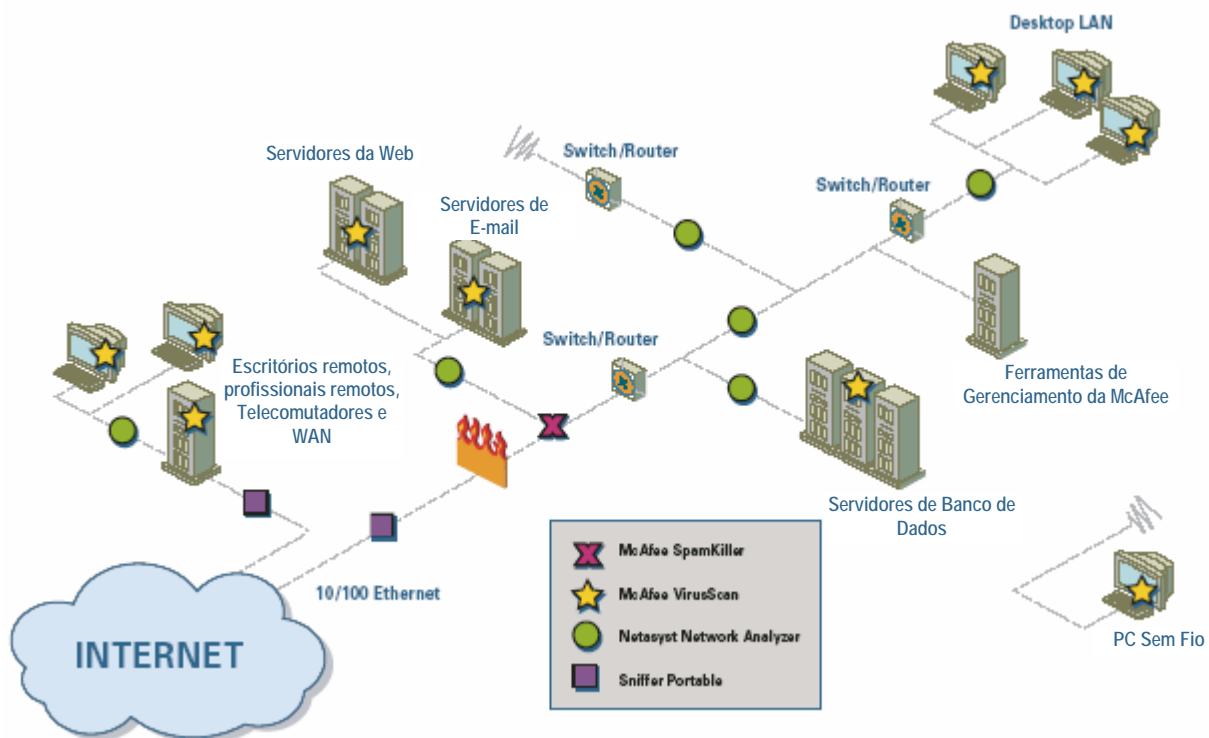
No processo de descoberta, não se espante com o fato de o acesso remoto ser sempre um ponto de vulnerabilidade, pois com o uso cada vez maior da Internet para viabilizar o acesso remoto, muitas vezes é difícil saber simplesmente quem está tentando entrar. Um firewall no ponto de entrada é obrigatório para a segurança da rede. Após a implementação dele, há diversas opções que podem ser usadas para promover o acesso remoto seguro. A opção mais comum colocada à disposição é a implementação de uma rede privada virtual (VPN), na qual todos os dados são criptografados e o acesso passa por um elaborado sistema de identificação que emprega chaves privadas específicas. Para garantir a maior eficiência da VPN, todos os sistemas remotos devem possuir um firewall pessoal.

Vírus e worms podem atacar pela Internet, por e-mail, ou por downloads da rede, e uma prática recomendada é equipar cada PC e estação de trabalho da rede com um sistema de detecção de vírus.

Entretanto, os hackers podem empregar outros métodos para atacar sua rede. O primeiro é um ataque de negação de serviço, pelo qual eles inundam os sistemas com solicitações de acesso até que estes não consigam mais dar conta. O segundo é um ataque que visa ao acesso para fins mal-intencionados. Em qualquer um dos casos, há produtos que podem ajudar a detectar esses ataques. Os sistemas de detecção de invasões de rede (NIDS) são famílias de produtos que monitoram continuamente o tráfego que chega à rede, capazes de detectar ataques à rede, analisá-los para determinar a melhor reação, com o intuito de bloquear ataques em andamento, e, finalmente, implementar políticas capazes de impedir antecipadamente as invasões no futuro. Para aumentar a velocidade e a eficiência, muitas vezes os sistemas são appliances de rede autônomos.

Com o acesso protegido no perímetro da rede, o próximo passo é pensar na rede corporativa. Para compreender os problemas de segurança da rede, é importante ser capaz de compreender os padrões de tráfego da rede em links de LAN e sem fio. Dessa forma, você poderá usar essas informações para determinar e solucionar diversas situações de segurança.

A análise do tráfego da rede pode identificar a presença de outros servidores não-autorizados. Normalmente, o excesso de tráfego na rede indica alguma forma de violação de segurança, seja ela causada por um worm, um vírus ou outra fonte mal-intencionada. Servidores, processadores ou usuários não-autorizados podem ser isolados da rede e análises mais minuciosas podem ser realizadas para estabelecer a raiz do problema.



As soluções da McAfee combinam-se para proporcionar segurança completa à rede

A maior parte das SMBs possui um servidor interno de e-mail implementado. Embora não se trate necessariamente de uma ameaça direta à segurança, o spam — mensagens de e-mail indesejadas que, segundo pesquisas internas, já responde por quase 50% de todos os e-mails — é uma ameaça geral à produtividade de toda a empresa. Uma solução anti-spam implementada no servidor de e-mail pode ser usada para reduzir consideravelmente ou eliminar o spam das caixas de correio de todos os usuários da rede.

A Network Associates pode ajudar você a aumentar a segurança de sua rede

A Network Associates oferece a melhor combinação de soluções de gerenciamento de segurança de sistemas e redes para SMBs por meio de duas famílias de produtos: McAfee® System Protection Solutions e McAfee Network Protection Solutions. O diagrama acima mostra algumas das soluções a seguir usadas simultaneamente para proporcionar total segurança à rede.

Soluções McAfee System Protection para empresas de pequeno e médio porte

Empresas de pequeno e médio porte são tão vulneráveis a vírus e hackers quanto as grandes empresas. Com os sistemas de negócios conectados à Internet, sua empresa está sempre à mercê de atividades mal-intencionadas, as quais podem derrubar os sistemas de computação, afetando negativamente os negócios ou simplesmente paralisando-os.

As soluções da McAfee ajudam a reduzir esses riscos com software e serviços projetados, levando sua pequena empresa em consideração. Eis algumas dessas soluções:

McAfee System Protection—Active Virus Defense Small Business Edition

A McAfee Security oferece proteção máxima contra vírus para empresas de pequeno e médio porte. Normalmente, as empresas com menos de 250 funcionários não possuem os recursos para um gerenciamento completo de antivírus. A McAfee Security soluciona esse problema com a Small Business Edition do Active Virus Defense, que conta com o McAfee VirusScan®, o WebShield® eo NetShield®, projetados para defender todas as camadas de sua rede. Além disso, ele integra o controle do ePolicy Orchestrator® (ePO™), que fiscaliza a política antivírus de sua preferência e oferece uma visibilidade sem precedentes da defesa antivírus em sua rede. O Active Virus Defense Small Business Edition evita epidemias, promove a produtividade e protege seu orçamento antivírus.

McAfee System Protection—VirusScan ASaP

O McAfee VirusScan ASaP é o serviço antivírus remoto líder de mercado que protege desktops e servidores continuamente contra códigos mal-intencionados, utilizando as proteções mais atualizadas. Usando a tecnologia de varredura de última geração da McAfee Security, o VirusScan ASaP detecta arquivos infectados acessados em desktops ou servidores, limpando-os, colocando-os em

quarentena ou excluindo-os automaticamente para proteger seu ambiente. Com suas atualizações automáticas, o VirusScan ASaP protege sistemas que não têm conexão com a Internet, podendo até mesmo distribuir proteção antivírus avançada a usuários de linhas discadas. Projetado para proteger até 200 mil computadores, o VirusScan ASaP permite que você delegue o ônus de gerenciar o software antivírus, reduz os custos operacionais e ajuda você a voltar a dedicar-se ao sucesso de seus negócios.

McAfee System Protection—McAfee SpamKiller for Microsoft Exchange

Ajustado para operar em alta velocidade, o McAfee Security SpamKiller® “powered by McAfee SpamAssassin™” oferece proteção incomparável para servidores Microsoft® Exchange 2000 e 2003, proporcionando até 95% de detecção de spam sem nenhum ajuste especial. O McAfee SpamKiller pode ajudar você a reduzir os custos associados à varredura do spam, aplicando a varredura aos e-mails assim que eles chegam ao servidor Exchange. Após a varredura, o spam pode ser colocado em quarentena em uma pasta de lixo eletrônico no servidor ou na pasta de lixo eletrônico do usuário. Ao detectar o spam, você evita que seus usuários precisem lidar com mensagens indesejadas, o que aumenta a produtividade deles.

Soluções McAfee Network Protection para empresas de pequeno e médio porte

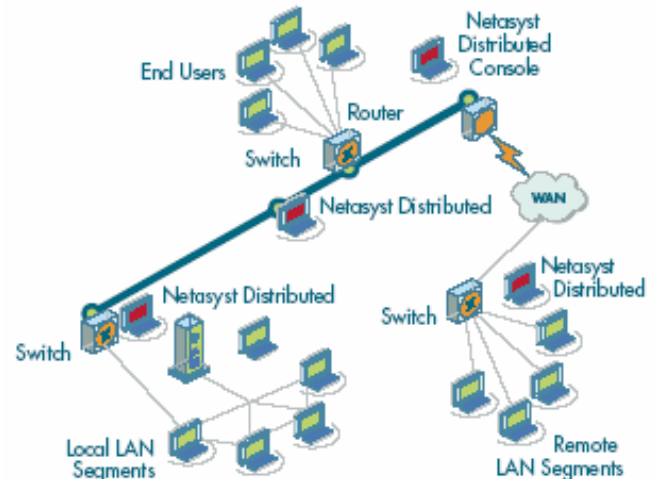
A família de soluções McAfee Network Protection foi criada para gerenciar e resolver proativamente os problemas de sua rede. Essas soluções oferecem vários produtos para o gerenciamento de sua rede. As soluções de proteção de rede que ajudam você a identificar e resolver problemas de maneira rápida, fácil, econômica e adequada são:

McAfee Network Protection — McAfee IntruShield 1200

O McAfee IntruShield® 1200 (I-1200) é um poderoso appliance sensor para detecção e prevenção contra invasão de redes que proporciona uma implementação econômica para redes de médio porte, de escritórios remotos ou de filiais. O gerenciamento centralizado pela Web para implementações de IDS em toda a empresa reduz drasticamente os custos operacionais. O I-1200 possui duas portas de detecção Fast Ethernet, exploradores de rede Fast Ethernet incorporados, uma porta Fast Ethernet para reação e outra para gerenciamento, além de operar a uma velocidade de até 100Mb/s.

McAfee Network Protection — Netasyst Network Analyzer Distributed

O software Netasyst™ Distributed é uma solução confiável, flexível e econômica para resolver problemas remotamente e gerenciar redes LAN 10/100 LAN. A solução pode ser instalada em PCs dedicados e implementada em toda a sua empresa em segmentos de LAN 10/100 para proporcionar uma visibilidade ininterrupta de sua rede. Com a interface de usuário (UI) no estilo Windows, você pode ter acesso a informações sobre a rede a qualquer momento, em qualquer



lugar, além de gerenciar proativamente toda a sua rede a partir de um único local. O Netasyst Distributed é uma solução “Powered by Sniffer Technologies” que utiliza os decodificadores e as análises avançadas que as grandes empresas vêm empregando para gerenciar, proteger e planejar o crescimento das redes pertencentes a essas corporações.

McAfee Network Protection — Netasyst Network Analyzer LAN

Os produtos Netasyst para LAN mantêm sua rede Ethernet 10/100 funcionando em velocidade máxima. O analisador captura pacotes, criando, ao mesmo tempo, um banco de dados de objetos de rede a partir do tráfego observado para detectar anomalias na rede. Após o Netasyst isolar, analisar e categorizar um problema, ele alerta você, explicando o problema e recomendando medidas de correção. O Netasyst utiliza o sistema Expert Analysis da Sniffer® Technologies para aprimorar a automação do gerenciamento, ampliar as informações sobre solução de problemas e aumentar a visibilidade da rede.

McAfee Network Protection — Netasyst Network Analyzer Wireless

Os produtos Netasyst para redes sem fio proporcionam uma solução abrangente para o gerenciamento de aplicativos e implementações em redes 802.11a e 802.11b. Com a capacidade de decodificar o tráfego com Privacidade Equivalente à de Redes Cabeadas (WEP), seja antes ou depois da captura, o Netasyst oferece a você uma incomparável flexibilidade para solucionar problemas. A análise avançada específica para ambientes sem fio permite que os produtos Netasyst para redes sem fio detectem rapidamente violações de segurança em radiofrequências por usuários móveis não-autorizados ou por pontos de acesso desprotegidos. Acompanhando todo o comportamento da rede sem fio e exibindo todas as informações conhecidas, os produtos Netasyst podem determinar rapidamente se um ambiente está sobrecarregado ou com um desempenho eficiente. Essa função garante a correção de problemas de velocidade, a

remoção de equipamentos sem fio desprotegidos e a descoberta de usuários móveis não-autorizados para que eles não representem mais uma ameaça à segurança da rede.

McAfee Network Protection — Sniffer Portable

Sniffer Portable é uma família de soluções para gerenciamento de falhas e desempenho de rede que permitem aos profissionais de rede manter, solucionar problemas, ajustar e expandir redes com várias topologias e vários protocolos. Essa solução portátil pode ser incluída em uma rede, onde quer que ela seja necessária para resolver problemas. Configure o software Sniffer Portable e as opções dele em questão de minutos para começar a controlar todas as informações que entram ou saem de sua rede por meio do gateway da Internet, e que trafegam nas sub-redes internas. Ele opera praticamente em todas as topologias de rede local (LAN) e rede remota (WAN), desde a Ethernet 10/100 até os mais recentes backbones ATM (Modo Assíncrono de Transferência) e Gigabit de alta velocidade. O software Sniffer Portable funciona em desktops, portáteis ou notebooks, podendo utilizar componentes de hardware avançados e personalizados para garantir recursos de captura em alta velocidade.

McAfee Network Protection — Sniffer Reporter

O Sniffer Reporter é um aplicativo opcional de emissão de relatórios que aprimora a solução Netasyst Network Analyzer. Também é oferecido acompanhando a solução Sniffer Portable. Ele gera relatórios gráficos com base nos dados coletados pelos produtos Netasyst e/ou Sniffer Portable. Relatórios predefinidos, fáceis de gerar, que exibem rapidamente estatísticas globais, tabelas de host e relatórios de matriz, bem como distribuição de protocolos no segmento de rede monitorado. Esses dados ajudam os gerentes de rede a projetar necessidades futuras de largura de banda e remanejar recursos de rede. Junto com a análise

avançada do Sniffer, o Sniffer Reporter identifica e corrige a degradação da rede antes que ela leve a uma grave indisponibilidade.

Resumo

Embora o quadro geral do gerenciamento da segurança de redes possa parecer assustador no início, subdividi-lo e analisar suas necessidades em todos os níveis reduz significativamente a complexidade. Além disso, a Network Associates possui uma gama completa de ferramentas confiáveis para ajudar você a manter sua rede com segurança máxima 24 horas por dia, 365 dias por ano.

Com ou sem fio, a montagem de uma rede pode levar sua SMB a um nível mais alto em termos de comunicações pela Internet, colaboração em tempo real, hospedagem da Web e comércio eletrônico — ou simplesmente ser configurada para conectar uma série de estações de trabalho a uma impressora compartilhada.

Empresas de pequeno e médio porte têm as mesmas necessidades de segurança das grandes empresas, mas não contam com recursos humanos que possam dedicar-se em tempo integral à tarefa. Sendo assim, o software desempenha um papel fundamental na implementação de uma rede segura e protegida. A Network Associates oferece as soluções McAfee System Protection (para proteger desktops e servidores) e as soluções McAfee Network Protection (para garantir a proteção e a velocidade da rede corporativa).

Não importa se seu escritório possui 25 ou 500 funcionários, nós da Network Associates entendemos que seus negócios dependem da segurança ininterrupta de sua rede, e o nosso compromisso é sermos um valioso aliado para manter sua rede operando sem problemas.

Então, PARE de se preocupar com segurança de sistemas e COMECE a pensar em aumentar a produtividade dos sistemas e usuários.

Se quiser obter mais informações sobre soluções para SMB, visite http://www.nai.com/us/audiences/small_buisness_home.asp.

McAfee Security 3965 Freedom Circle, Santa Clara, CA 95054, 800.338.8754

Os produtos da Network Associates® trazem com eles anos de experiência e compromisso com a satisfação do cliente. A equipe PrimeSupport®, composta de atenciosos e altamente qualificados técnicos de suporte, oferece soluções sob medida, proporcionando assistência técnica detalhada para gerenciar o sucesso de projetos fundamentais — tudo com níveis de serviço para atender às necessidades de cada empresa cliente. A McAfee® Research, líder mundial em sistemas e segurança da informação, continua na vanguarda das inovações no desenvolvimento e refinamento de todas as nossas tecnologias.

Network Associates, McAfee, VirusScan, WebShield, NetShield, ePolicy Orchestrator, ePO, SpamKiller, Powered by SpamAssassin, IntruShield, Netasyst, Sniffer e PrimeSupport são marcas comerciais, registradas ou não, da Network Associates, Inc. e/ou de suas afiliadas nos EUA e/ou em outros países. Os produtos que levam a marca Sniffer® são produzidos exclusivamente pela Network Associates, Inc. Todas as outras marcas comerciais, registradas ou não, apresentadas neste documento pertencem exclusivamente aos seus respectivos titulares. ©2004 Networks Associates Technology, Inc. Todos os direitos reservados. 6-net-smb-001-0304