Tudo que Você Precisa Saber Sobre Segurança de Rede

Introdução

Toda empresa já sentiu os benefícios da rede: processos internos mais rápidos, comunicações dinâmicas, produtividade aumentada para usuários remotos e móveis, e a conquista real de um mercado global. Assim que a empresa compreende o poder do comércio pela Internet, dos recursos de um escritório virtual e da resposta imediata de um escritório remoto, a sua demanda por acesso aumenta. As tendências-chave que levam ao crescimento espantoso da Internet como ferramenta de negócios inclui:

Força de Trabalho Crescendo Constantemente

As empresas estão dependendo cada vez mais do seu quadro de pessoal móvel para continuarem competitivas. O pessoal de vendas precisa ter acesso rápido a arquivos corporativos. Muitas vezes o vendedor de sucesso é aquele que pode processar uma proposta ou um pedido com rapidez, sem ter que esperar pelo correio. Nossa economia global exige funcionários capazes de conduzir os negócios de qualquer lugar, a qualquer hora. Outros funcionários, incluindo funcionários remotos e contratados, demandam ambiente de trabalho flexível, no qual possam executar seus trabalhos da comodidade de um home Office (escritório em casa).

Desenvolvimento das Extranets

É preciso haver uma interação on-line cada vez maior entre as empresas, seus fornecedores e parceiros. A tecnologia baseada na Web, como navegadores e servidores, está se tornando um meio comum para organizar e trocar informações. As indústrias se consolidam e formam alianças, as extranets permitem que duas empresas compartilhem informações e colaborem em seus projetos. Fazendo uso da Internet e tecnologias baseadas na Web, as empresas podem fornecer serviços a clientes autorizados com facilidade, rapidez e sem grandes investimentos.

Necessidade de uma Alternativa para Linhas Arrendadas

Antes, empresas que desejassem estabelecer uma rede privada não tinham outra escolha senão usar uma linha dedicada, que precisava ser arrendada de uma companhia telefônica. Pesquisas recentes estimam que as empresas podem economizar até 70% sobre o custo das linhas arrendadas (Pesquisa Forrester). A tabela seguinte compara as vantagens da VPN (Virtual Private Network) sobre aquela alternativa:

Linha arrendada tradicional	Rede Virtual Privada
Despesas mensais com longa distância	Pagamento só pelo uso real
Despesa significativa com equipamento – bancos de modem separados, adaptadores de terminais, servidores de acesso remoto, etc.	Reduzido investimento em equipamento - clientes/servidores, tokens (opcional)
A Interface pode ser de difícil aprendizado e uso	Interface simplificada, familiar ao usuário
Incompatível com os sistemas de clientes, fornecedores e parceiros confiáveis	Compatibilidade instantânea

O Risco com a Segurança Também Cresce

Quanto mais complexa se torna a rede, maior é o desafio para mantê-la segura. Com a expansão contínua da infra-estrutura da Internet e computação móvel, multiplicam-se os pontos de acesso a dados corporativos através da Internet e linhas de telefone dial-up. Cada ponto de acesso representa uma possível vulnerabilidade que pode ser aproveitada para conseguir acesso não autorizado à sua rede.

As ameaças dos hackers são lendárias, mas a realidade é ainda mais assustadora. Em um recente estudo feito pela InternetWeek, 60% dos entrevistados declarou que foram acessados de fora mais de 30 vezes. E os riscos são altos: estima-se que a perda de produtividade ou de informação vital resultante dessas quebras de segurança custe aos negócios mais de $5 bilhões por ano.

Proteger a propriedade intelectual e ao mesmo tempo permitir acesso transparente ao pessoal autorizado é o dilema do CIO (Diretor-Chefe de Informação) e a dor de cabeça do administrador da rede. Como se conectar com segurança à Internet? Como proteger dos hackers, concorrentes e vândalos eletrônicos suas fontes de informação vital? Como se conectar com segurança a outras organizações ou mesmo a outras sub-redes? Como ter certeza de que somente pessoas autorizadas estejam acessando sua informação? Por onde começar?

O primeiro passo é formular uma política de segurança, identificando os principais recursos a serem protegidos, e definir quem terá acesso aos mesmos. Este processo ajudará a estabelecer objetivos de segurança e a fazer um plano para administrá-los. Este guia tratará de segurança na Internet e do perímetro, delineando os pontos-chave de segurança que toda empresa precisa seguir para ter uma conexão segura com a Internet, mas você precisa conceber uma estratégia bem acabada que reúna as quatro categorias de proteção da informação: Avaliar, Proteger, Habilitar e Gerenciar.

- **AVALIAR** vulnerabilidades e assegurar o cumprimento da política.
- **PROTEGER** sistemas de informações críticas.
- **HABILITAR** o uso seguro da Internet.
- **GERENCIAR** e administrar usuários e recursos.

Todo empreendimento – emergente ou multinacional estabelecido, tem necessidades de segurança que vão além do acesso não autorizado através da rede pública. Conquanto ameaças externas de hackers sejam bem reais, ataques de funcionários descontentes são na verdade muito mais comuns e tipicamente mais prejudiciais. Desenvolver uma estrutura de segurança significa mais do que implementar um perímetro forte e a defesa da Internet. Requer uma abordagem de proteção tanto aos recursos vitais como de apoio às necessidades do negócio em todos os níveis do empreendimento.

Symantec do Brasil - Av. Dr. Chucri Zaidan, 920 - 12 º andar - Market Place Tower
São Paulo – SP - CEP: 04583-904 - Tel.: (11) 5189 6200 Fax: (11) 5189 6210
informe@symantec.com

Segurança do Perímetro

Pense na sua rede corporativa como sendo sua fortaleza. Para protegê-la de invasores, você precisa primeiro construir uma muralha impenetrável ao seu redor. Você abaixa e eleva a ponte levadiça, permitindo a entrada somente daquelas pessoas que se identificaram corretamente usando uma senha secreta. De tempos em tempos, você faz uma inspeção na fortaleza para assegurar-se de que não há brechas ou buracos que possam ser utilizados por saqueadores que pretendem ganhar acesso. E, por fim, você instala uma sentinela no topo da fortaleza para manter uma vigilância contínua, soar o alarme quando da aproximação de problemas e disparar flechas incendiárias para repelir intrusos astutos que se atrevem a escalar as muralhas da fortaleza.

Primeiro Passo: Proteger o Perímetro com um Firewall Impenetrável

Sua primeira linha de defesa dentro do empreendimento é proteger o acesso da e para a Internet. Sem essa proteção, a porta aberta para a Internet também é a porta aberta para a sua rede corporativa. Um Firewall efetivamente coloca uma barreira entre a rede corporativa e o lado externo, protegendo o perímetro e repelindo hackers. O firewall age como um único ponto de entrada, através do qual todo o tráfego que chega pela rede possa ser auditado, autorizado e autenticado. Qualquer atividade suspeita – baseada em normas que você estabelece – dispara um alerta.

Como escolher um Firewall

Na avaliação de um Firewall, é importante levantar todas essas questões:

- Como são criadas as regras?
- Oculta endereços de rede?
- Suporta autenticação segura?
- É multi-residente para proteger de ataques à Web e os servidores de correio da rede?
- Filtra Java e ActiveX?
- Como estabiliza o sistema operacional?
- Pode lidar com todo o seu tráfego de rede sem sacrificar a segurança?
- Fornece registro e alarme?
- É fácil de usar?
- Suporta softwares adicionais de relatório?
- Fornece bloqueio de conteúdo?
- É modular para acomodar futuras necessidades?
- Firewalls de sites remotos e usuários móveis podem ser facilmente acrescentados?
- É interoperável com outros produtos do mercado?

Symantec do Brasil - Av. Dr. Chucri Zaidan, 920 - 12 º andar - Market Place Tower
São Paulo – SP - CEP: 04583-904 - Tel.: (11) 5189 6200 Fax: (11) 5189 6210
informe@symantec.com

Tipos de Firewalls

Hoje em dia, há três tipos básicos de firewalls no mercado, cada um oferecendo diversos graus de segurança e flexibilidade: roteadores, pacotes de sistemas stateful de filtragem, e proxy firewalls em nível de aplicativo. Um simples roteador, conquanto barato, é inaceitável para a maior parte das necessidades do negócio. Roteadores não podem proteger contra ataques em nível de rede, tais como instrução enganosa de IP, roteamento de fonte, TCP SYB Flood, Ping of Death ou outros ataques não relacionados com a autorização das conexões. Roteadores também não oferecem o nível de flexibilidade e características de um firewall de total segurança para a empresa, como capacidade de rede virtual privada, registro e autenticação. Sistemas stateful examinam pacotes individuais imediatamente antes ou na camada da pilha de protocolo. Isto acelera o processamento de regras e evita que pacotes não associados com conexões já estabelecidas consigam atravessar. Em contrapartida, firewalls em nível de aplicativo autorizam conexões e examinam o fluxo de dados, forçando todo o tráfego de rede a passar por um aplicativo inteligente que é executado no sistema de firewall específico para esse serviço (FTP, HTTP, SMTP, etc). Esta forma de proxy lhe dá controle sobre funções em nível de aplicativo e fornece proteção contra ataques, prioridades absolutas para quase todas as organizações. Enquanto muitos dos sistemas stateful incluem uma limitada tecnologia proxy, a maioria não protege contra ataques incorporados no fluxo do aplicativo, como sobrecarga do buffer e comandos de aplicativo inseguros ou ilegais. Firewalls em nível de aplicativo, por outro lado, são projetados para frustrar os ataques incorporados mais sofisticados, incluindo aqueles que transpõe múltiplos pacotes de rede.

Fatores a Considerar:

Interfaces de Rede

A maioria dos firewalls de aplicativos proxy é multi-residente, para criar uma separação física entre a rede protegida e a rede não confiável. É desejável ter pelo menos três interfaces de rede para proteger contra ataques a Web pública e servidores de correio desta rede. Alguns firewalls podem se conectar diretamente à Internet através ISDN (Integrated Services Digital Network) integrado ou conexões Frame Relay, eliminando a necessidade de um roteador externo separado. Esta proteção confiável, inatacável, garante que tráfego não autorizado não passe pelo Firewall.

Tradução e/ou Ocultamento de Endereços

Seu firewall deve ser capaz de traduzir os endereços IP de origem e/ou destino do seu endereço original para outro diferente. A tradução é exigida por duas razões. A primeira é ocultar todos os endereços internos da rede. Esconder os endereços assegura que potenciais atacantes tenham pouca ou nenhuma informação sobre seus sistemas internos que pudesse ser usada para atacá-los. A segunda é que a tradução ajuda a preservar o espaço do endereço. É muito difícil conseguir uma escala completa de endereços registrados IPv4 da Internic. Através do ocultamento/agrupamento de endereços, é possível usar somente alguns endereços registrados para representar todos os sistemas de computação que estão atrás do firewall.

Em função do uso de proxies, firewalls em nível de aplicativo traduzem automaticamente todos os endereços internos para um único endereço externo ou registrado. Firewalls de filtragem de pacote precisam ser explicitamente programados para traduzir e/ou ocultar endereços, tarefa essa monótona e tediosa.

Criação de Regras de Acesso

O firewall segue um conjunto de regras que você configura de acordo com a sua política de segurança. Estas regras autorizam o reconhecimento e o fluxo de tráfego baseado no host e nos endereços de rede, e outros parâmetros tais como uma escala de data e hora. A segurança do seu firewall depende muito da sua habilidade de configurar apropriadamente estas regras. Se você configurá-las incorretamente, pode inadvertidamente criar um buraco na segurança.
A maioria dos firewalls utilizam regras próprias, dependentes de ordens. É notoriamente fácil configurar de maneira errada estes sistemas dependentes de ordens. Se o administrador não for extremamente cuidadoso no estabelecimento da política, ou se posteriormente adicionar dados, o ordenamento incorreto das regras pode abrir uma brecha séria na segurança. Alguns firewalls empregam regras não dependentes de ordens, mais ajustadas, para simplificar enormemente a criação de políticas e eliminar o risco de erro do operador. Regras de acesso mais ajustadas eliminam a possibilidade de uma regra substituir e anular outra inadvertidamente, criando um buraco na segurança. À medida que suas necessidades de segurança crescem e se tornam mais complexas, este tipo de firewall apresenta flexibilidade para adicionar regras de maneira simples e sem risco de desconfiguração. Sistemas abrangentes mais ajustados são mais intuitivos e mais fáceis de gerenciar, resultando em um sistema firewall mais seguro.

Estabilização do Sistema Operacional

Para dizer o mínimo, o seu firewall deveria oferecer alguma forma de estabilização do sistema operacional quando o firewall for instalado. Idealmente, esta estabilização deve ser totalmente automática, e não exigir grandes configurações manuais, o que aumenta o risco de erro do operador. Alguns firewalls oferecem estabilização automática do sistema operacional na instalação e durante o funcionamento. Estes firewalls monitoram o sistema operacional continuamente para garantir o seu correto funcionamento.

Velocidade/Desempenho

O seu firewall age como um gateway para todas as comunicações de entrada e saída de sua rede corporativa, autenticando usuários, codificando e decodificando mensagens e roteando-as dentro da sua rede. O firewall precisa controlar rigidamente a segurança, ao mesmo tempo em que controla o tráfego de centenas de usuários, sem desacelerar o tráfego de rede. Uma vez que os firewalls de filtragem de pacotes não reconhecem toda e qualquer conexão, historicamente eles apresentam desempenho um pouco melhor, sem sacrifício da segurança.

Autenticação

O seu firewall deve ser capaz de autenticar usuários que estão tentando se conectar com a sua rede. A maneira mais simples é através de uma senha. Em alguns casos, não é possível autorizar baseado somente no endereço IP (devido ao DHCP – Dynamic Host Configuration Protocol) ou não é suficientemente seguro (devido a endereços IP externos facilmente enganáveis). Um firewall pode fornecer autenticação para serviços tais como FTP, HTTP e Telnet de maneira que somente usuários específicos ou grupos de usuários tenham permissão de acesso de uma rede para outra.

Tokens de autenticação verificam a identidade e autorizam acesso aos usuários da rede de acordo com a sua política. Estes esquemas geram uma nova senha a cada login para eliminar a ameaça de ataques repetitivos de senha.

Registro

Um registro de cada tentativa de conexão ao ou através do firewall. Inclui as tentativas bem e mal sucedidas. O registro dá ao administrador um relatório não confiável do que ocorreu. Também pode ser usado para rastrear de que forma uma empresa está usando a Internet. Um relatório adequado inclui itens tais como data/hora, endereços IP de origem e destino, nomes de usuários, tipo de serviço (FTP, HTTP, etc.) e arquivos ou URLs transferidos. Alguns firewalls têm capacidade para desabilitar o registro, o que é enfaticamente desencorajado, uma vez que seria impossível reconstruir ou rastrear uma atividade de ataque quando esta ocorrer.

Alerta

O alerta é um mecanismo que notifica o administrador sempre que o firewall exige atenção. Isto é feito tipicamente através de e-mail, pager, armadilhas no SNMP (Simple Network Mangement Protocol) e/ou mudança de estado do sistema firewall, tocando arquivos de som ou mudando as cores da tela. Qualquer firewall, na melhor das hipóteses, só pode suspeitar da ocorrência de um ataque (se soubesse quando ocorreu a penetração, em primeiro lugar teria impedido o ataque). O alerta é uma maneira de informar o administrador sobre atividade incomum ou suspeita.

Serviços de Rede Virtual Privada

Os serviços de rede virtual privada permitem que empresas com várias fábricas/escritórios estendam sua rede além dos limites físicos e forneçam comunicações seguras para o quadro de venda móvel ou para escritórios remotos de filiais. Serviços VPN (Virtual Private Network) integrados ao firewall facilitam o gerenciamento da política de segurança a partir de um local e uma interface de usuário.

Adaptabilidade

Procure um firewall que se adapte totalmente às suas necessidades futuras, seja para uma atualização do hardware, gerenciamento da segurança em um site remoto, adicionar um quadro de vendedores móveis, ou interoperar com os sistemas de seus parceiros comerciais. Sistemas não-patenteados que utilizam hardware e sistemas operacionais padrão, geralmente constituem a melhor abordagem, permitindo reutilização quando o firewall precisar ser substituído. Procure características de interoperabilidade, cruciais para a integração do seu sistema de firewall a ambientes mistos. O cumprimento de padrões industriais assegura interoperabilidade com seus fornecedores, clientes e sócios estratégicos aos quais você pode querer estender o acesso à rede.

Bloqueadores de Conteúdo

A Internet fornece muita informação útil, que também favorece o mau uso. Alguns firewalls oferecem mecanismos de bloqueio integrados, que permitem restringir a navegação de material não produtivo ou questionável da Web ou grupos de notícias. Estes filtros permitem que você dê aos seus funcionários o acesso à Internet de que necessitam, e ao mesmo tempo reforça as políticas corporativas.

Segundo Passo: Verificar a Segurança do Perímetro

Quando o firewall estiver instalado e configurado, o próximo passo é testá-lo a fundo para ter certeza que não foram inadvertidamente criados ou deixados buracos comprometedores ou pontos fracos que poderiam ser explorados. Uma vez que redes são complexas e mudam com freqüência, tais testes de penetração deverão ser executados rotineiramente.
Você poderia contratar um "tiger team" dispendioso para fazer os testes de penetração; você pode fazer isto uma vez, mas certamente não poderá arcar com essa despesa todos os meses. Uma ferramenta de sondagem (probe) é uma escolha mais eficiente e de custo mais baixo. Ferramentas de sondagem verificam as formas comuns de penetração em redes e analisam o risco de cada vulnerabilidade detectada. Algumas ferramentas de sondagem fazem verificação automática de vulnerabilidade tanto do perímetro como da rede interna, avaliam riscos e até fornecem conselhos abalizados com respeito aos problemas de segurança encontrados. Como resultado, é possível localizar rapidamente buracos na rede e fechá-los, antes que os dados sejam furtados ou danificados.

Como Escolher uma Ferramenta de Sondagem

Certifique-se que a sonda escolhida verifica vulnerabilidades não só de dentro do firewall, mas também de fora, o que espelhará o ponto de vista do hacker acerca da vulnerabilidade da sua rede. Escolha um verificador que empregue múltiplos protocolos – não somente IP – para detectar recursos de rede vulneráveis, tais como NetWare, que pode ser acessado sem ser via IP. Anteriormente, estes verificadores só eram capazes de sondar uma única caixa por vez. Hoje em dia, já existem produtos sofisticados para testar múltiplos sistemas ao mesmo tempo, revelando como vulnerabilidades pequenas podem ser exploradas em conjunto, criando um importante risco de segurança.

Terceiro passo: Instalar uma Sentinela

Enquanto um firewall alerta sobre atividade suspeita, mas nada faz para interrompê-la. Tentar revisar manualmente todos os arquivos de registro leva um tempo enorme e é uma batalha. A instalação de um detector de invasão lhe concede uma medida de proteção adicional.
Um detector de invasão age como sentinela para guardar o perímetro e imediatamente detectar e responder a ataques na rede. A principal função da detecção de intrusão não é impedir a invasão, mas capturar a invasão e interrompê-la antes que algo possa acontecer. Algumas das reações automáticas peculiares incluem notificação ao administrador de segurança, interrupção da seção ofensiva, fechamento do sistema, desligamento de links da Internet, desativação de usuários; ou a execução de um procedimento de comandos pré-estabelecidos. Detectores de invasão oferecem proteção 24 horas por dia, 7 dias por semana.

Como Escolher uma Solução para Detecção de Invasão

Um método efetivo para detecção de invasão em tempo real é monitorar a atividade relacionada à segurança que ocorre nos diversos sistemas e dispositivos que formam a rede. Enquanto a maioria dos monitores de atividade vigiam as trilhas de auditoria do sistema operacional, as ferramentas mais sofisticadas também:

- Companham trilhas de auditoria de aplicativos, base de dados, servidores Web, roteadores, firewalls, etc.
- Monitoram arquivos críticos em busca de Trojans, modificações não autorizadas, etc.
- Vigiam atividade da porta UDP (User Datagram Protocol) e TCP (Transfer Control Protocol)
- Aceitam armadilhas SNMP e gatilhos

Monitores de atividade em tempo real podem detectar ataques, tais como tentativas de acesso não autorizado a arquivos, ou substituir um programa de login por uma nova versão. Diferentemente dos farejadores (sniffers) de pacotes, podem detectar quando um usuário obtém ilegalmente acesso de administrador ou de “raiz”. Quando uma atividade suspeita é detectada, os monitores de atividade em tempo real podem tomar providências imediatas antes que ocorram danos. A vantagem do monitoramento de atividade em tempo real está na sua implementação perto dos dados e aplicativos críticos da missão. Monitoramento contra ataques de dentro e de fora da rede se torna mais fácil, pois todos os dispositivos estão sendo vigiados. Adicionalmente, muitos ataques no nível dos aplicativos e dos sistemas operacionais não são discerníveis no nível do pacote e para sua detecção exigem monitoramento no nível de sistema. Ao escolher um detector de invasão, procure um que possa ser gerenciado a partir de um console central, e que ao mesmo tempo monitore as atividades de toda a rede. Eventos que conseguem atravessar pelo dispositivo são então avaliados por um detector de invasão. Atividades suspeitas de múltiplas posições na rede devem estar correlacionadas à medida que ocorrem. Por exemplo, um invasor pode usar um programa de hacker para tentar adivinhar a senha raiz em cem sistemas UNIX ao mesmo tempo.

O software precisa ter capacidade para detectar invasão, mesmo que as conexões de rede estejam codificadas ou que os atacantes utilizem conexões dial-up diretas. O detector deverá registrar atividades de segurança críticas em sistemas gerenciadores. Este procedimento dificulta aos hackers encobrirem suas pistas, uma vez que a atividade está registrada em outro sistema na rede – e não somente em uma trilha de auditoria local. Também centraliza e facilita o gerenciamento de trilhas de auditoria. Por fim, como novos ataques estão sendo criados diariamente, o detector de invasão deverá ser de fácil atualização para controlar novos cenários regularmente. O fornecedor deverá publicar estes cenários na Web de maneira que você possa copiá-lo e implementá-lo rapidamente por toda empresa.

Quarto Passo: Impedir Acesso Não Autorizado via Dial-Up

A última peça na segurança de perímetro é impedir acesso não autorizado à sua rede. Sem autenticação, um hacker pode facilmente simular usuários legítimos para conseguir acesso à rede corporativa. Como é possível garantir acesso dos usuários remotos aos recursos de que necessitam para fazer o seu trabalho sem sacrificar a segurança da rede corporativa? Você determina se o usuário é quem ele diz ser, solicitando alguma forma de autenticação. Hoje em dia há dois tipos básicos de esquemas de autenticação em uso nos sistemas de operação, servidores de comunicação, e firewalls:

- Senha estática (hard-coded)
- Autenticação de dois fatores (forte)

IDs e senhas estáticas tradicionais provaram ser inadequadas para autenticar usuários de modo único. Senhas estáticas são facilmente conhecidas por terceiros, compartilhadas, adivinhadas e quebradas. A obrigação do usuário de trocar regularmente suas senhas faz com que eles escolham senhas de fácil conhecimento e risco. Em virtude do grande número de senhas a serem lembradas, elas também podem ser anotadas e deixadas à vista. As senhas também podem ficar comprometidas por ferramentas de hackers, tais como farejadores de senhas, ataques de dicionário, etc. Com as senhas roubadas, fica fácil simular os usuários legítimos e acessar os arquivos.

Autenticação de Dois Fatores (Two-Factor)

Sistemas de autenticação de dois fatores somente autenticam usuários, sem forçá-los a lembrar uma nova senha. A autenticação de dois fatores é baseada na informação de algo de posse exclusiva do usuário – um token – e algo de conhecimento exclusivo do usuário – um número PIN para ativar o token. Este processo cria uma senha exclusiva para ser usada uma única vez, que não pode ser adivinhada, compartilhada ou quebrada. Por essa razão, a autenticação de dois fatores é altamente preferível a outros esquemas menos seguros.

Tokens de Software vs Tokens Portáteis
Tokens de software e tokens portáteis são igualmente seguros e cada um tem suas vantagens. Tokens de software são ideais para usuários que empregam um único dispositivo para se conectar na rede, enquanto que tokens portáteis são mais úteis a usuários que se conectam com freqüência de diferentes posições e plataformas. Tokens portáteis podem ser facilmente perdidos ou furtados e custam o dobro dos tokens de software. Por outro lado, os tokens de software são mais fáceis de usar por serem transparentes para o usuário. Além disso, eliminam a necessidade de carregar um token portátil separado. O laptop ou PC do usuário se transforma em um token quando o token de software é ativado.

Segurança Internet & Extranet

Ao mesmo tempo em que o baixo custo e a disponibilidade da Internet a tornam uma atraente ferramenta de negócios, ela é uma rede pública que não oferece segurança. As comunicações pela Internet são extremamente arriscadas sem a tecnologia adequada. E-mail, arquivos e senhas são facilmente interceptados por uma variedade de "farejadores" e ferramentas de hackers. Na verdade, muitas ferramentas de hackers estão disponíveis na Internet gratuitamente. Como você protege dados sensíveis de bisbilhoteiros enquanto eles viajam pela Internet? Uma vez que a Internet pode ser usada como um meio para estender a sua rede corporativa literalmente à qualquer lugar, com uma boa relação custo/benefício. Como você pode estabelecer uma rede privada segura para seus múltiplos sites, usuários remotos, e "guerreiros da estrada" distribuídos pelo mundo? Navegadores e servidores baseados na Web permitem centralizar informações e serviços – como você pode estender um acesso seletivo a seus parceiros comerciais, fornecedores e clientes, sem comprometer a segurança?

Primeiro Passo: Implementar uma Rede Virtual Privada

O que é uma Rede Virtual Privada?

A rede virtual privada combina autenticação com codificação de dados e autorização para proteger a informação ao longo do seu trajeto pela Internet pública.
A tecnologia VPN:
1. Estabelece um túnel seguro entre o usuário remoto e a rede corporativa
2. Encapsula e codifica pacotes de dados
3. Autentica o usuário e autoriza acesso dos usuários aos recursos corporativos na rede.

Codificação

Antes da transmissão, os dados são codificados e encapsulados para protegê-los de bisbilhoteiros. As informações destes pacotes codificados não podem ser visualizadas, modificadas ou interceptadas de forma utilizável. Além disso, as informações interceptadas não fornecem qualquer informação útil sobre o host protegido de uma rede corporativa. Ela utiliza poderosos algoritmos de codificação, de padrão industrial, para garantir que os dados que viajam pela Internet, WANs, redes de clientes ou Intranet não sejam interceptados. O produto escolhido deve suportar um algoritmo de codificação forte, "forte" em relação à sensibilidade dos seus dados. A maioria dos fornecedores oferece como opção uma chave de codificação de 40-bits. O comprimento da chave de 40-bits foi escolhido porque o governo dos Estados Unidos

permite exportar esta codificação sem controle de exportação. A codificação de 40 bits interromperá crackers acidentais, mas não deve ser considerada forte.
Na codificação que utiliza o padrão Data Encryption Standard de 56 bits, ou DES, os algoritmos são aproximadamente 65.000 vezes mais fortes do que os algoritmos de 40 bits. Apesar da recente publicidade envolvendo o esforço coroado de êxito para invadir uma mensagem curta DES, para a maioria dos propósitos o DES é considerado muito forte. Para uso nos Estados Unidos e Canadá, podem ser utilizados algoritmos ainda mais fortes. De maneira geral, estes algoritmos, tais como Triple-DES, utilizam comprimentos mais longos de chave para dar maior proteção.

Segundo Passo: Identificar Quem Acessa a Informação

Produtos de rede virtual privada precisam fornecer um meio de garantir, ou autenticar, a identidade do usuário. A autenticação tradicional depende de senhas estáticas ou reutilizáveis. Estas senhas são facilmente obtidas pelos hackers e são, muitas vezes, deixadas à vista anotadas em Post-Its, na agenda ou na carteira do usuário. A autenticação forte, ou de dois fatores, apresenta o mais alto nível de segurança a acesso remoto, sem sobrecarregar os usuários com senhas adicionais ou procedimentos de login. Além disso, fornece mecanismos de alta confiabilidade para responsabilização do usuário. Quando entra a linha de comando, o usuário digita seu PIN para abrir uma caixa de diálogo de autenticação forte, transparente entre o usuário e a rede. Os dados trocados durante uma interação pedido de senha/resposta são válidos apenas uma vez, e o PIN do usuário nunca é transmitido pela rede pública. Mesmo que a troca seja interceptada por qualquer número de técnicas de hacking, não é mais válida para acesso.

A autenticação é inútil se o seu usuário tentar tomar um atalho. Quanto mais fácil de usar, maiores as chances de não ser contornado, comprometendo a segurança. Os melhores esquemas de autenticação consolidam o número de passos sign-on, permitindo ao usuário simplesmente entrar um ID e senha após o login em um laptop ou PC. O PIN do usuário é a única exigência necessária para ativar um acesso remoto seguro. A autenticação forte, de dois fatores, é executada de maneira transparente para o usuário final. A autenticação não é usada somente para verificar a identidade de um indivíduo, mas para determinar a que recursos ele terá acesso. Por exemplo, seus funcionários remotos e móveis podem ter acesso à mesma quantidade de informações disponíveis para seus funcionários internos: informações financeiras, sobre a concorrência e sobre produtos. Seus parceiros comerciais, por outro lado, podem ter acesso somente a informações específicas relacionadas a um projeto conjunto, mas precisam montá-las a partir de informações financeiras ou da concorrência. E você pode dar aos seus clientes acesso exclusivo a serviços específicos baseados na Web, mas não a detalhes confidenciais do seu negócio. Cada um desses usuários exige uma estratégia de segurança diferente: remota, móvel e extranet.

Terceiro Passo: Controle de Acesso Remoto

Usuários remotos em várias filiais exigem o mesmo nível de segurança utilizado na sede corporativa. Isto significa fortificar os seus perímetros com um firewall, fazendo verificações rotineiras com uma ferramenta de sondagem, e instalando um detector de invasão de resposta preventiva a invasores. Cada firewall pode ser ligado (linked) através da rede virtual privada. Procure um firewall que ofereça soluções VPN integradas e suporte a múltiplos firewalls remotos. Gerenciamento centralizado através do firewall corporativo oferece flexibilidade e proteção máximas, além de economia. Os firewalls remotos oferecem, em princípio, um produto com a mesma funcionalidade, menos a interface de gerenciamento.

Quarto Passo: Controle de Acesso Móvel

O software cliente da VPN é executado no laptop ou PC do usuário. O servidor pode estar integrado a um firewall ou residir em um gateway que fica atrás do firewall. Há vantagens e desvantagens em ambos. Software dependente de firewall garante compatibilidade do firewall com o cliente VPN. VPNs múltiplos são gerenciados a partir de um console de firewall central. Em contrapartida, software VPN independente de firewall é vantajoso para os gerentes de rede com muitos tipos de firewalls incompatíveis e, por ser independente do firewall, não tem impacto sobre o seu desempenho. VPNs múltiplos são gerenciados de maneira centralizada através da interface de servidor VPN. O crescente número de laptops furtados preocupa muito.

De acordo com a Safeware Insurance, uma das maiores seguradoras de computadores, foram comunicados os furtos de mais de 250.000 laptops em 1996, representando um aumento de 27% sobre 1995, e uma perda de mais de $800 milhões em bens de hardware e software. Cada notebook de negócios contém informação proprietária, que varia de dados sobre contatos com clientes a informações financeiras. Como é possível proteger as informações nos laptops de usuários remotos? Os produtos VPN têm codificação de arquivos local para assegurar que os dados do PC não possam ser vistos por usuários não autorizados. Arquivos sensíveis são codificados e decodificados. Muitas soluções de codificação em desktop exigem codificação ou decodificação dos dados a cada vez que determinado arquivo é acessado. Quase todos os usuários, muitas vezes por pressa, não lembram de executar esse passo, deixando os dados desprotegidos, apesar do software estar em seu laptop. Alguns produtos fazem isso automaticamente, protegendo sem esforço os dados armazenados nos laptops dos atarefados usuários finais. Arquivos recém-criados são automaticamente protegidos, não importando onde os arquivos são criados e guardados (localmente, em servidores de arquivos, disquetes ou até mesmo transmitidos por rede). A proteção de estações de trabalho inativas controla PCs desacompanhados que são deixados ligados ou conectados à rede, exibindo o protetor de tela do Windows após determinado período de tempo, requerendo do usuário um novo logon para ganhar acesso ao sistema.

Quinto Passo: Acesso Remoto Seguro à Web

As empresas estão rapidamente implementando aplicativos baseados na Web como um meio conveniente de publicar informações e acessar serviços corporativos, tornando-os disponíveis em uma posição central. Os seus aplicativos Web fornecem acesso a informações empresariais valiosas e são visitados com freqüência. Infelizmente, servidores Web são recursos críticos que se tornam bons alvos para hackers internos. Como é possível estender o acesso aos seus clientes, fornecedores e parceiros sem comprometer a segurança? Com uma audiência tão diversificada acessando informações baseadas na Web, como é possível controlar e gerenciar quem visita e que informações tem permissão para acessar? Conseguir controle de acesso seguro e centralizado a informações baseadas na Web é particularmente desafiador, dadas as limitações da atual tecnologia Web. Embora a combinação de um navegador e um servidor Web constitui um veículo de comunicação poderoso, grande parte da atual tecnologia desenvolvida para a Web, como por exemplo cookies, não foram projetados para segurança e escalabilidade. Servidores múltiplos requerem autenticação e administração individuais, e múltiplos serviços mantêm seus próprios meios de rastreamento e precisam ser gerenciados separadamente. Já está disponível uma nova tecnologia de segurança de Web para fornecer administração baseada na Web logo que a embalagem é aberta. As características que devem ser procuradas na avaliação de tecnologia de segurança na Web incluem:

Escalabilidade

O sistema de controle de acesso a implementar deve ser independente da arquitetura do aplicativo Web e possuir uma interface de administração centralizada fácil de usar. Isto permite aos projetistas da Web reutilizar os aplicativos Web para fazer frente a exigências de expansão sem ter que refazer a engenharia do sistema de controle de acesso. E também elimina a necessidade de ter que se fazer um novo treinamento dos administradores do site.

Sign-on único para controle de acesso seguro

Para ser um controle de acesso seguro, a arquitetura de uma ferramenta deve incluir um servidor central para solicitar credenciais aos usuários e ratificar métodos de autenticação existentes ou diretórios de usuários por eles utilizados. Deverá fornecer um mecanismo para administrar “tickets” (bilhetes de entrada) para transportar a informação de autorização do usuário e não requerer autenticação posterior.

O usuário precisa de um navegador padrão Web e, uma vez que as comunicações ocorrem na Internet, o administrador de segurança precisa ter a flexibilidade de codificar toda troca de informação durante a autenticação.

Após a autenticação e do “bilhete de entrada” inicial, o usuário pode se movimentar dentro do site da Web e acessar o conteúdo permitido pelo administrador de conteúdo, sem necessidade de autenticação adicional para aquela sessão. Todavia, se os “tickets” forem usados para armazenar informação de acesso do usuário no navegador da Web, o sistema de controle de acesso precisa lidar com dois problemas de segurança. Primeiro, ele precisa impedir que algum hacker, que pode ter conseguido um ticket “farejando” a rede, modifique este ticket para conseguir acesso. Segundo, ele precisa garantir que o administrador possa especificar um dado período de tempo para a validade deste ticket. A exposição da proteção da autenticação do nome/senha do usuário pode ser evitada com o uso de ferramentas que requerem apenas um

sign-on para acessar aplicativos Web. O risco do usuário armazenar múltiplas senhas difíceis de lembrar em posições não seguras fica assim eliminado (por exemplo em blocos de notas próximos aos seus computadores ou em suas agendas), onde podem ser facilmente localizados e "furtados". Ademais, utilizar ferramentas que requerem validação da senha apenas no início e uma única vez, reduz o risco de hackers "farejarem" nomes e senhas de usuários quando estes são transmitidos pela rede.

Gerenciamento de Segurança Centralizado

Soluções que fazem controle centralizado podem suavizar estas frustrações para os gerentes e usuários finais. Os administradores de segurança precisam de aplicativos de controle de acesso que ofereçam uma interface gráfica de usuário (GUI) para selecionar métodos de autenticação, configurar e gerenciar o acesso de usuários em um ou mais servidores Web. Ademais, como a maioria das corporações também tem Webmasters e administradores de conteúdo separados para cada servidor mais importante, o aplicativo de controle de acesso deve fornecer não somente uma interface de administração de segurança centralizada, mas também permitir aos administradores de conteúdo separados aplicar os diretórios específicos de proteção de acesso e conteúdo que eles gerenciam. Isto é particularmente importante, uma vez que o conteúdo da Web é, em geral, extremamente dinâmico e os privilégios consignados aos usuários não são estáticos.

Interoperabilidade

Ao selecionar ferramentas de proteção de acesso à Web, devem ser consideradas aquelas que oferecem suporte multi-plataforma. Uma ferramenta deve oferecer controle de acesso centralizado para servidores Web NT e UNIX, protegendo desta forma conteúdo baseado em UNIX com credenciais de domínio NT. À medida que o seu site na Web se tornar ainda mais bem sucedido, serão adicionados novos serviços e o tráfego irá aumentar. Você precisa de uma solução que se adapte às suas crescentes necessidades. Abordagens tradicionais falham em um ambiente de plataforma cruzada. Dependem de servidores Web, Secure Socket Layer (SSL), codificação e programação de aplicativos que muitas vezes degradam e restringem a utilização de aplicativos Web e podem abrir – em vez de fechar – a porta para acesso não autorizado. Escolha uma tecnologia de segurança da Web que se instale e se integre totalmente com as plataformas e infraestruturas de segurança existentes, utilizando padrões de segurança e protocolos Web para comunicação entre componentes.

Suporte de Sistema de Múltipla Autenticação

Usuários devem ter flexibilidade para exigir senhas tradicionais reutilizáveis para autenticação ou requerer autenticação forte de token antes de acessar os serviços da Web.

Soluções de Segurança Symantec

As organizações estão modificando suas maneiras de fazer negócios. Com o advento da Internet, elas estão mudando das tradicionais paredes físicas de uma corporação, para uma corporação "virtual". E conforme as organizações modificam seus modelos para alavancar os benefícios de e-business e e-commerce, a segurança da rede se torna um facilitador de negócios. As soluções de e-security da SYMANTEC são a resposta para ajudar os clientes a fazerem frente às novas necessidades de adaptação a novos modelos de negócios. E-security é a capacidade de gerenciar riscos de bens de informação e facilitar processos de negociação com segurança, ajudando os clientes a maximizarem vantagens de negócio. Como parceiro de segurança confiável a SYMANTEC fornece e-security para avaliar, proteger, habilitar e gerenciar processos de negócio e bens de informação através da nossa abordagem exclusiva Lifecycle Security. Para ajudar a identificar necessidades de segurança e implementar soluções de segurança práticas, a SYMANTEC desenvolveu o modelo Lifecycle Security Model. Este modelo elimina hipóteses, oferecendo uma abordagem estruturada para projetar, implementar e gerenciar a segurança em todo o seu empreendimento.

Como chave do Lifecycle Security Model, a SYMANTEC oferece soluções Lifecycle Security para:
-AVALIAR vulnerabilidades e assegurar o cumprimento da política
-PROTEGER sistemas de informações críticas
-HABILITAR o uso seguro da Internet.
-GERENCIAR e administrar usuários e recursos.

Avaliar

O primeiro passo para reduzir ativamente riscos corporativos é medir eficazmente o cumprimento de uma política de segurança da empresa e avaliar vulnerabilidades inerentes a informações críticas. É importante entender a eficácia de uma política de segurança, agora e à medida que muda com as necessidades da empresa, de maneira a poder definir, gerenciar e impor políticas de negócio e avaliar possíveis ameaças.

Enterprise Security Manager™

O ESM é uma solução de gerenciamento de segurança em nível empresarial que define, gerencia e impõe sua política de segurança da informação. O Enterprise Security Manager verifica ativamente vulnerabilidades de segurança em todo o empreendimento, avalia riscos de segurança, e controla de forma centralizada os parâmetros de segurança de mais de 55 plataformas.

NetRecon™

O NetRecon é uma ferramenta de terceira geração para análise de risco e vulnerabilidade de rede que descobre relatórios e explora buracos na segurança da rede. Diferentemente de "scanners de segunda geração" mais velhos, o NetRecon aplica uma tecnologia exclusiva, de patente pendente, que opera com uma abordagem de colaboração de um "tiger team".

Symantec do Brasil - Av. Dr. Chucri Zaidan, 920 - 12 º andar - Market Place Tower
São Paulo – SP - CEP: 04583-904 - Tel.: (11) 5189 6200 Fax: (11) 5189 6210
informe@symantec.com

Proteger

As organizações precisam proteger as informações contra usuários indesejados e hackers e controlar o acesso às informações para manter a integridade do negócio. Equilibrar essas necessidades requer um conjunto de soluções que protejam os dados de dentro do perímetro, verifiquem e detectem ataques ao perímetro e controlem o acesso à informação, para assegurar aos clientes que os dados proprietários estão seguros.

Intruder Alert

O Intruder Alert detecta e reage a quebras na segurança e atividades suspeitas de fora do perímetro, assim como de dentro. O Intruder Alert monitora sistemas e redes em tempo real para detectar quebras na segurança e atividades suspeitas e reage automaticamente, de acordo com a política de segurança estabelecida. Funciona por todo o empreendimento, incluindo LANS, WANs, intranets e a Internet.

NetProwler™

O NetProwler oferece detecção dinâmica de invasão à rede que examina de forma transparente o tráfego da rede para instantaneamente identificar, se conectar e finalizar o uso não autorizado, mal uso ou abuso de sistemas de computadores por sabotadores internos ou hackers externos. O seu processador virtual SDSI, de patente pendente, possibilita o desenvolvimento imediato de assinaturas de ataque personalizadas para terminar até mesmo as mais sofisticadas violações de segurança.

Symantec Enterprise Firewall

O Symantec Entreprise Firewall combina o mais alto nível de segurança de perímetro disponível com o desempenho, interoperabilidade, escalabilidade e facilidade de uso para ir de encontro aos objetivos do seu negócio. Este premiado firewall oferece segurança empresarial centralizada e em tempo real por toda Internet, intranets, computação móvel e sites remotos, para dar aos usuários autorizados acesso total e seguro à rede. Symantec Entreprise Firewall inclui o primeiro e único servidor VPN certificado IPSec™ para Windows NT®.

Habilitar

A Internet é um recurso fundamental que faculta às organizações uma comunicação mais eficiente, uma redução nos custos com telecomunicações e provê informações em tempo oportuno. É crítico entregar informações a funcionários, parceiros e clientes pela Internet sem comprometer a segurança desta informação. A Internet pode ajudar a viabilizar novas oportunidades de negócio e reduzir custos operacionais.

Defender

O Defender ajuda a reduzir o risco de invasões indesejadas através da Internet com seu sistema de autenticação de dois fatores, que cria senhas de uso único que autenticam exclusivamente usuários e concedem acesso por dial-up, ISDN, Internet e conexões Rede Local.

PassGo™ InSync

O InSync fornece sincronização de senha empresarial de maneira rápida e segura. O PassGo InSync pode ser facilmente implementado, produzindo como benefício imediato o aumento da

produtividade por meio da sincronização de senha de um único uso que pode se estender à múltiplos sistemas, servidores, redes e aplicativos.

PassGo SSO

O PassGo SSO dá ao usuário um único ponto de acesso às informações críticas da empresa. PassGo SSO é uma solução de administração flexível, totalmente personalizável, que confirma as credenciais do usuário com o Authentication Service (Serviço de Autenticação), que é usado por todas as plataformas para controlar acesso à rede e aos aplicativos.

WebDefender™

O WebDefender fornece controle de acesso sign-on único e seguro através de um número crescente de aplicativos Web e servidores Web da empresa. O WebDefender centraliza o gerenciamento da autenticação e autorização do usuário final, para reduzir o custo de implementação dos seus aplicativos Web.

Soluções VPN

As Soluções VPN da Symantec conectam com segurança usuários remotos, escritórios de filiais e terceiros aos aplicativos e dados da sua rede corporativa. Ao contrário dos produtos VPN tradicionais, que oferecem somente sessões codificadas, as soluções VPN da SYMANTEC permitem ao gerente da rede controlar, colocar na tela e definir minuciosamente quando e qual informação uma pessoa tem permissão para acessar.