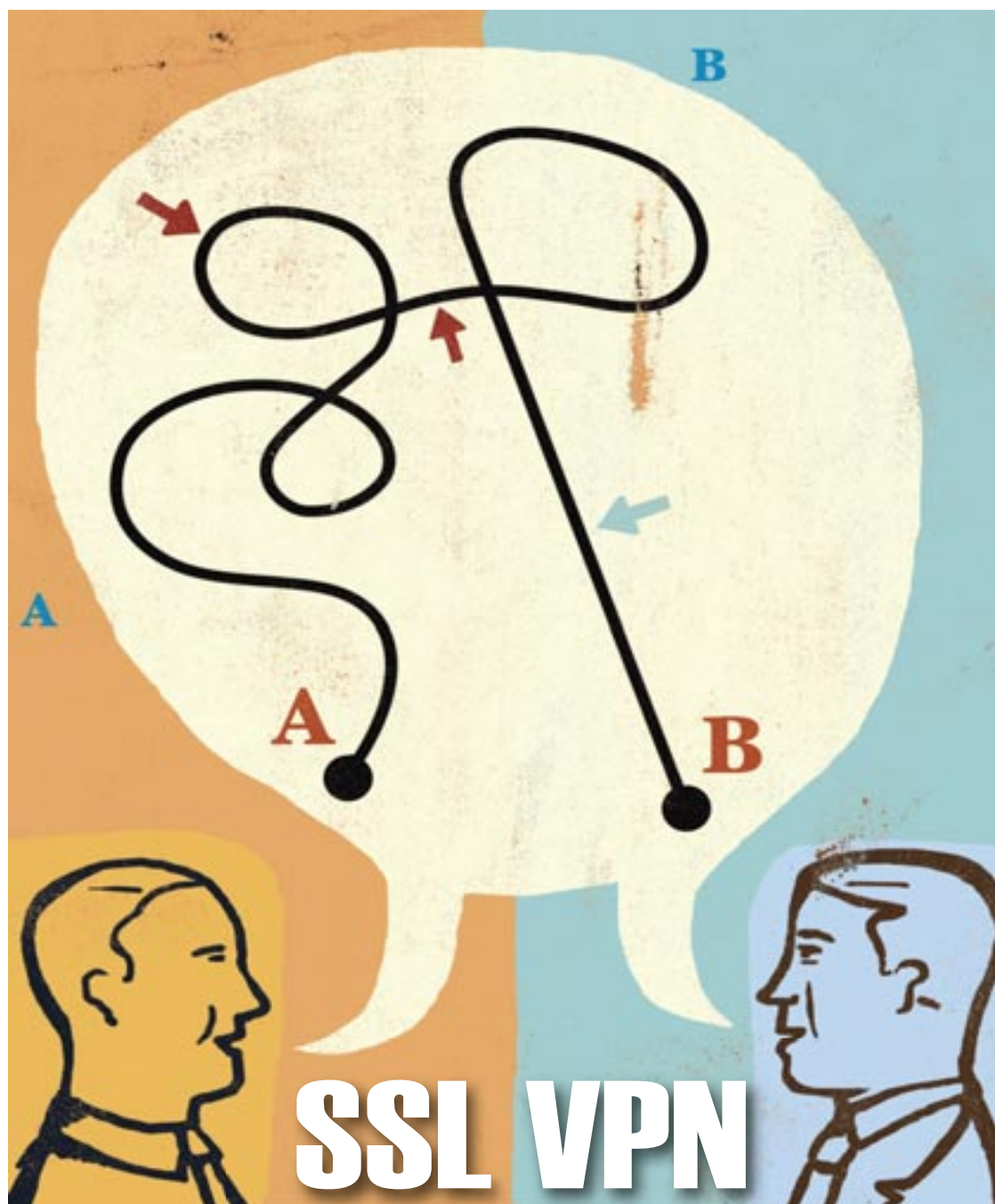


COMPUTERWORLD

Março 2010

O protocolo Secure Sockets Layer (SSL), que começou por ser um modo de assegurar a segurança das transacções de comércio electrónico, tornou-se uma alternativa de baixo custo ao protocolo IPsec utilizado nas redes privadas virtuais. Ligar computadores pessoais remotos de um modo seguro às redes de comunicações corporativas, estes equipamentos implementam SSL, que não é um protocolo único mas um conjunto de rotinas de transferência desenhadas para proteger a integridade das mensagens transmitidas. O protocolo SSL baseia-se em certificados – cartões digitais de identificação – e chaves. Os certificados incluem o nome da autoridade que emitiu o certificado, o nome da entidade a que foi atribuído o certificado, a chave pública da entidade e selos com os dados de expiração do certificado.

A simplicidade do protocolo SSL traduz-se na facilidade de instalação e redução de custos no longo prazo devido a um suporte mais simples, por oposição ao protocolo IPsec VPN que requer um cliente IPsec dedicado em cada equipamento remoto.



➔ Olá SSL VPN. Adeus, IPsec VPN

O protocolo SSL VPN representa uma das grandes histórias de sucesso tecnológico da última década, destronando a indústria estabelecida em redor do protocolo IPsec VPN.

Pág. 2

➔ Como adquirir uma SSL VPN

As considerações seguintes podem auxiliar a determinar quando a tecnologia SSL VPN é a melhor opção para acesso remoto seguro.

Pág. 3

➔ Boas práticas: implementar SSL VPN

Suporte a autenticação e a uma variedade de clientes é crucial para o sucesso destas implementações.

Pág. 4

➔ Acesso remoto simplificado

A tecnologia SSL VPN permite a ligação segura de equipamentos remotos a redes de comunicação através da evocação do protocolo SSL.

Pág. 4

Olá SSL VPN. Adeus, IPsec VPN

O mercado dos protocolos SSL VPN é uma história de sucesso.



O protocolo SSL VPN representa uma das grandes histórias de sucesso tecnológico da última década, destronando a indústria estabelecida em redor do protocolo IPsec VPN e, recentemente, adquirindo o negócio de acesso remoto. O seu sucesso foi tão completo que as tecnologias IPsec VPN saíram do radar das organizações que procuram conselho junto do Gartner Group. “Os clientes do Gartner já não fazem perguntas sobre novas instalações de acesso remoto com tecnologias IPsec ou pela expansão dos acessos remotos IPsec”, refere um estudo da empresa.

As empresas que mantêm o protocolo IPsec VPN para acesso remoto fazem-no porque já está instalado e ainda não alcançou o fim de vida. Ou mantêm-no para uma utilização específica e limitada, geralmente por profissionais de TI que necessitam de entrar na rede de comunicações para corrigir algumas situações e necessitam de acesso total à rede.

Alguns clientes do Gartner interromperam as novas implementações de acesso remoto baseadas em protocolo IPsec, assim como outros abandonaram o protocolo IPsec e substituíram pelo protocolo SSL, citando benefícios de facilidade de provisionamento administrativo das contas de utilizador e uma experiência simplificada dos utilizadores nas sessões VPN, refere o estudo do Gartner.

As empresas estão interessadas na tecnologia SSL VPN porque os browsers podem detectá-la. Isto torna esta tecnologia mais flexível do que o protocolo IPsec, que requer um cliente de software separado nos equipamentos remotos, sublinha o estudo do Gartner.

Esta adaptação a evolução das necessidades de negócio, como a crescente utilização de consultores e alianças mais amplas que requerem a partilha de recursos de rede com os parceiros. As empresas que rely em trabalhadores móveis ou pessoas que trabalham a partir das suas residências e que podem não ter acesso a equipamentos geridos pela empresa foram responsáveis pela popularidade da tecnologia SSL VPN.

“A tecnologia SSL VPN substituiu o protocolo IPsec como a escolha mais fácil para acesso casual e ad hoc dos empregados a VPN e para parceiros de negócio, fornecedores de manutenção exteriores e associados reformados”, refere o estudo do Gartner.

A tecnologia SSL VPN é ainda atractiva porque, com a descarga dos agentes SSL VPN, podem duplicar o nível de rede suportado pelo protocolo IPsec VPN se for aquilo que os clientes querem. Sem estes agentes, utilizando apenas um browser ou equipamentos remotos, a tecnologia SSL VPN pode estabelecer ligações ao nível do ‘layer’ de aplicações.

Quando as VPN baseadas na Internet apareceram no final da década de 90, o seu objectivo era óbvio: era mais barato adquirir acessos Internet e criar ligações WAN do que adquirir circuitos dedicados, ou serviços frame relay ou MPLS. Apesar de, presentemente, as suas vantagens serem óbvias, a tecnolo-

gia SSL teve que travar uma dura luta para se estabelecer como uma inovação requerida.

A tecnologia SSL é uma norma que assegura comunicações seguras e encriptadas entre aplicações e a criação de ligações seguras entre ‘browsers’ e servidores Web é a sua utilização mais popular. A tecnologia SSL é independente dos protocolos subjacentes, incluindo IP. Por outro lado, o a tecnologia IPsec é uma colecção de normas que também suportam Comunicações seguras e encriptadas no ‘layer’ IP. A tecnologia IPsec é independente das aplicações, pelo que uma aplicação IP pode ser executada através de um túnel IPsec.

A restrição da tecnologia SSL de apenas poder suportar aplicações Web foi um obstáculo inicial. Como a tecnologia SSL VPN requeria apenas um browser, as empresas deixaram de necessitar de distribuir e manter software cliente nos equipamentos remotos, na medida em que os clientes apenas necessitavam de aceder a aplicações Web. Tal afastou alguns dos potenciais clientes cujos utilizadores necessitavam de aceder a aplicações cliente-servidor tradicionais. Mas o crescimento da utilização de aplicações Web e a adopção de ‘front-ends’ Web nas restantes aplicações aumentou o sucesso da tecnologia SSL. Os fabricantes de tecnologias SSL VPN adaptaram-se através da instalação de agentes SSL VPN em Java ou em Active X nos equipamentos remotos. Estes componentes permitiram aos equipamentos remotos a capacidade de criar ligações ao ‘layer’ de rede comparáveis ao protocolo IPsec, mas sem ter que distribuir software cliente para VPN dedicadas.

O crescimento das redes Wi-Fi no interior das organizações empresariais veio auxiliar a penetração da tecnologia SSL VPN. Com os problemas de segurança das redes Wi-Fi que possibilitaram a entrada ilegal nas redes corporativas, os especialistas em segurança pensaram um meio de reduzir o acesso através dos pontos de acesso wireless.

Como as VPN preenchiam os requisitos porque podiam ser adicionadas às implementações wireless existentes para autenticar utilizadores na rede de comunicações e encriptar o tráfego à medida que viajava pelo ar. As SSL VPN eram atractivas porque não necessitavam de software cliente.

Os problemas inerentes ao protocolo IPsec contribuíram para o sucesso da tecnologia SSL. O protocolo IPsec foi sempre complexo. Quanto mais sites se ligavam uns aos outros, mais túneis de segurança necessitavam, de ser definidos e mantidos. E existia ainda questões da instalação e manutenção dos clientes.

A utilização de equipamentos não geridos para aceder a VPN SSL deu lugar a tecnologias que analisam os pontos de acesso antes de ter acesso VPN para determinar qual o seu grau de confiança. Esta tecnologia foi o embrião das tecnologias de Network Access Control (NAC), cujo desenvolvimento pretendeu assegurar que os equipamentos ligados à rede de comunicações estavam conformes com as políticas de segurança corporativa. ■ CW

➔ Como adquirir uma SSL VPN

Os testes permitem identificar indicadores para escolher o produto adequado.

As considerações seguintes podem auxiliar a determinar quando a tecnologia SSL VPN é a melhor opção para acesso remoto seguro:

- ➔ Ligações originárias de um 'browser'.
- ➔ O departamento de tecnologias de informação tem um controlo limitado sobre o sistema remoto ou sobre o software cliente, como seja o caso dos parceiros ou dos clientes.
- ➔ A empresa necessita de disponibilizar acesso de curta duração e ocasional a partir de computadores residenciais, aeroportos, quiosques ou cafés Internet.
- ➔ Os requisitos de acesso remoto incluem acesso a recursos de rede limitados.
Quando considerar implementações SSL VPN, analise estas questões em primeiro lugar:
- ➔ Os custos de formação são reduzidos? A maioria das tecnologias SSL VPN possuem suporte dos 'browsers' comerciais.
- ➔ Suporta os métodos de autenticação existentes e planeados? Os componentes de software e os equipamentos SSL suportam os métodos de autenticação existentes, assim como autenticação mútua utilizando certificados digitais.
- ➔ Disponibiliza acesso em qualquer local? A tecnologia SSL pode ser evocada através de um 'browser' a partir de qualquer computador pessoal em qualquer localização – um quiosque numa feira, um café Internet, hot-spots Wi-Fi, outra rede corporativa e qualquer computador com acesso à Internet. No entanto, é importante referir que se deve ter cuidado a assegurar que estes locais não estão comprometidos com software malicioso, como malware, spyware ou key loggers, tornando estes locais inseguros.
- ➔ Como é que reduzi as questões de interoperacionalidade da rede? Na medida em que o protocolo subjacente é o mesmo utilizado para tornar as transacções Web seguras, uma VPN SSL funciona a partir de qualquer localização comum 'browser' Web, incluindo ambientes empresa-parceiros e através de servidores 'proxy', sem alterar a infraestrutura de segurança subjacente.
- ➔ Disponibiliza ubiquidade de clientes? O software de cliente está inserido no 'browser' Web instalado na generalidade dos equipamentos dos utilizadores, eliminando a necessidade de instalar software VPN cliente.

Desvantagens da tecnologia SSL VPN

Algumas implementações SSL exigem certas precauções para proteger as credenciais de segurança do utilizador remoto. Por exemplo, numa ligação pública Internet, quando um utilizador efectua actividades bancárias através da Internet, todos os dados devem ser limpos adequadamente após o encerramento da sessão. De outro modo, existem oportunidades para tentativas maliciosas de recolher dados após o utilizador finalizar a transacção bancária.

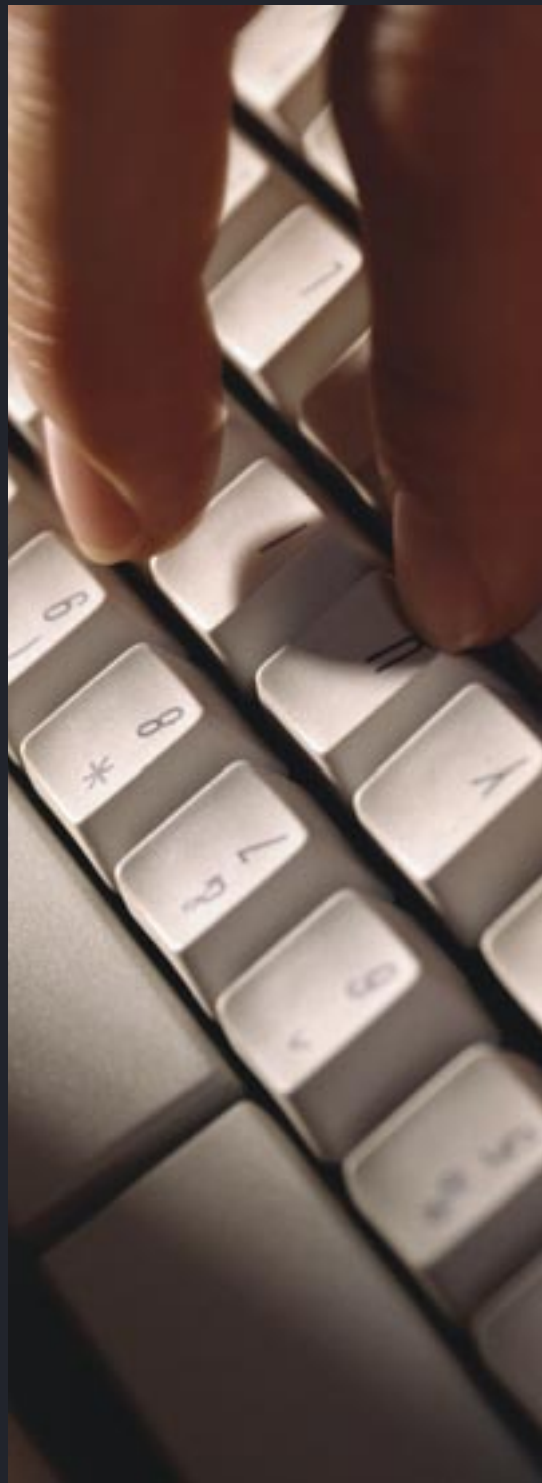
Não ter a necessidade de instalar um cliente VPN é uma das vantagens associadas à utilização das tecnologias SSL VPN, mas em simultâneo somente as aplicações acessíveis através da Web podem utilizar a tecnologia SSL com o protocolo de segurança. Existem desenvolvimento nesta área para possibilitar aos utilizadores uma experiência no interior da organização em SSL tornando outras aplicações seguras.

Os locais comprometidos na Internet podem receber sinais encriptados SSL da Internet para iniciar actividade não ética, como seja um ataque distribuído de negação de serviço.

As VPN baseadas na tecnologia SSL são uma nova tecnologia que disponibiliza conectividade para acesso remoto a partir da maioria dos locais com acesso Internet utilizando a encriptação nativa SSL incluída nos 'browsers'. Apesar da acessibilidade aplicacional estar restringida relativamente ao protocolo IPSec VPN, as VPN baseadas em SSL permitem acesso a um crescente número de aplicações de software.

Estas VPN requerem pequenas alterações ao fluxo de trabalho dos utilizadores porque algumas das aplicações são apresentadas através de uma interface Web, e não através da sua interface gráfica nativa. O suporte a aplicações cliente/servidor requer 'applets' específicas que sejam descarregadas para o sistema remoto.

Utilizar tecnologia Web para conectividade permite a acessibilidade a partir de quase todos os sistemas Internet sem necessidade de instalar software adicional no computador pessoal. Na medida em que as VPN baseadas na tecnologia SSL podem disponibilizar acesso de rede a utilizadores a partir de qualquer sistema ligado à Internet, começa a ser uma opção emergente para ampliar o acesso remoto a utilizadores que requerem acesso a aplicações específicas. ■ CW



COMPUTERWORLD

PROPRIEDADE  workmedia

RUA GENERAL FIRMINO MIGUEL, Nº 3 TORRE 2 - 3º PISO 1600-100 LISBOA DIRECTOR EDITORIAL: TIMÓTEO FIGUEIRO tfigueiro@computerworld.workmedia.pt EDITOR: JOÃO PAULO NÓBREGA jnobrega@computerworld.workmedia.pt DIRECTOR COMERCIAL E DE PUBLICIDADE: PAULO FERNANDES pfernandes@computerworld.workmedia.pt TELEF. 210 410 329 – FAX 210 410 303 DIRECTOR DE ARTE: JOSÉ TEIXEIRA zteixeira@workmedia.pt TODOS OS DIREITOS SÃO RESERVADOS.



O Computerworld, detém um acordo de licenciamento com a IDG, o líder mundial em media, estudos de mercado e exposições na área das tecnologias de informação (TI). Fundada em 1964, a IDG possui mais de 9.000 funcionários em todo o mundo. A IDG oferece o mais vasto leque de opções de media, os quais atingem consumidores de TIs em mais de 90 países, os quais representam 95% dos gastos mundiais em TIs. O portfolio de produtos e serviços abrange seis áreas chave: publicações impressas, publicações online, exposições e conferências, estudos de mercado, formação, e serviços de marketing globais. Mais de 90 milhões de pessoas lêem uma ou mais das 290 revistas e jornais da IDG, incluindo as pertencentes às principais famílias -Computerworld, PC World, Network World, Macworld e Channel World. A IDG Books Worldwide é o editor de livros de informática com mais rápido crescimento a nível mundial, com mais de 700 títulos em 38 línguas. Só a série "... For Dummies" tem mais de 50 milhões de cópias em impressão. Através da IDG.net (<http://www.idg.net>), a IDG oferece aos utilizadores online a maior rede de sites Internet especializados em todo o mundo. Esta compreende mais de 225 sites Internet em 55 países. A International Data Corporation (IDC) é o maior fornecedor mundial de informações sobre TIs, de análise e consulta, possuindo centros de pesquisa em 41 países e mais de 400 analistas em todo o mundo. A IDG World Expo é um produtor de primeira linha de mais de 168 conferências e exposições com marca própria, abarcando 35 países e incluindo a E3 (Electronic Entertainment Expo), Macworld Expo, ComNet, Windows World Expo, ICE (Internet Commerce Expo), Agenda, DEMO, and Spotlight. ExecuTrain, a subsidiária de formação da IDG, é a maior empresa do mundo na área da formação em informática, com mais de 230 instalações em todo o mundo e 785 cursos. A IDG Marketing Services ajuda empresas de topo na área das TIs a construir uma imagem reconhecida internacionalmente. Para isso desenvolve programas globais de marketing integrado, através das exposições e das suas publicações impressas e online. Pode encontrar mais informações do grupo IDG no site www.idg.com.

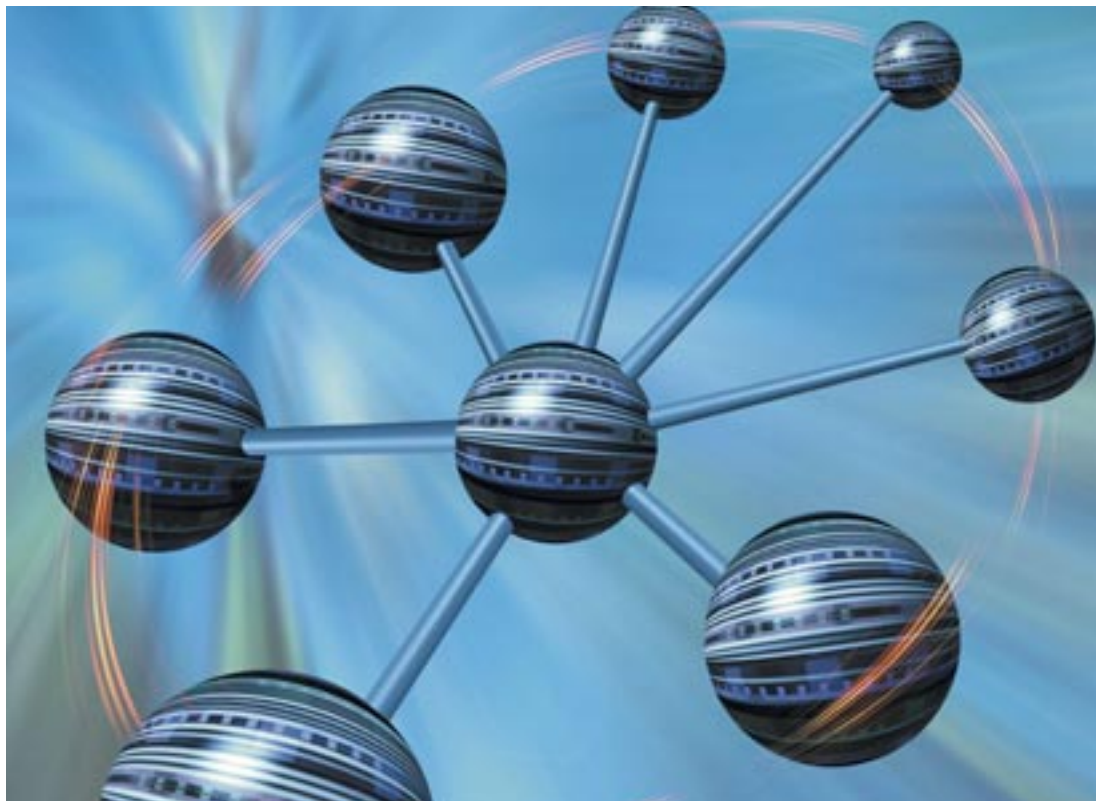
Boas práticas para implementar SSL VPN

Suporte a autenticação e a uma variedade de clientes é crucial para o sucesso destas implementações.

- Uma das razões para utilizar a tecnologia SSL VPNs é a de permitir aos utilizadores a ligação através de equipamentos que não sejam da empresa. Este é um objectivo importante, pelo que deve identificar se o produto avaliado suporta os sistemas operativos Windows, Linux e Mac e ainda sistemas operativos dos 'handhelds' e de 'smartphones' equipados com 'browsers'.
- Analise a plataforma de gestão e a sua capacidade de suportar múltiplas políticas por utilizador e por grupo de utilizadores. Na medida em que a tecnologia suporta acesso granular, pode ser desejável definir mais do que uma política por pessoa ou por grupo. Por exemplo, um utilizador pode requerer direitos de acesso que diferem consoante o equipamento ou o método de acesso utilizado e qual a postura de segurança do equipamento.
- Para reforçar a segurança, utilize autenticação de dois factores para aceder à VPN.
- Utilize opções que apaguem do equipamento remoto quaisquer traços das transacções efectuadas no decorrer de uma sessão SSL VPN. Isto é particularmente importante se a empresa não for proprietária do equipamento remoto e este está acessível a outros, como um computador num quiosque Internet.
- Utilize opções que obrigam as sessões a ser interrompidas e exija reautenticação para prevenir acessos não autorizados em caso dos utilizadores terem abandonado o equipamento deixando-o vulnerável à utilização de terceiros.
- Pondere a importância do acesso SSL VPN para o negócio. Se é essencial, instale gateways no modo de alta disponibilidade, para que se um gateway falhar, poder rapidamente ser substituído por outro.
- Se a tecnologia SSL VPN for utilizada para acesso à rede de Comunicações em caso de desastre, implemente a capacidade de suportar carga adicional. Se o 'gateway' não estiver configurado para suportar utilizadores adicionais, passará a ser outro problema quando o desastre ocorrer.
- Execute testes de penetração na VPN. Esta tecnologia, que deverá ser segura, permite o acesso a recursos corporativos, mas é necessário verificar. ■ CW

Acesso remoto simplificado

Como funciona a tecnologia SSL VPN.



A tecnologia SSL VPN permite a ligação segura de equipamentos remotos a redes de comunicação através da evocação do protocolo SSL que autentica os equipamentos e encripta as comunicações. Não existe uma norma SSL VPN, pelo que os fabricantes implementam estas VPN de modos diferenciados, mas aqui fica uma descrição de como funcionam.

O primeiro passo está relacionado com o 'browser' do equipamento remoto que se liga ao gateway SSL VPN. Este equipamento encontra-se no interior do firewall corporativo e actua como um interface com os servidores. O utilizador autentica-se no 'gateway' utilizando qualquer dos métodos de acesso e é-lhe conferido o acesso.

Como parte do processo de autenticação, o 'gateway' pode analisar o equipamento remoto para determinar se é um equipamento gerido. Se for este o caso, 'o gateway' pode analisá-lo para identificar se o equipamento está em conformidade com as políticas de segurança da rede. Estas análises podem identificar se o equipamento possui um firewall correctamente configurado ou o software antivírus activo.

Os equipamentos que não são geridos podem não permitir estas análises e são classificados como estado de conformidade desconhecido.

O 'gateway' pode ainda determinar como o equipamento está a tentar ligar-se à rede de Comunicações, seja através da Internet, através da rede local

ou através de um ponto de acesso Wi-Fi.

O gateway compila todos estes factores para determinar o estado de segurança do utilizador, o equipamento utilizador o método de acesso. Baseado nos resultados da autenticação, as políticas predefinidas ditam se o utilizador pode ter acesso e que tipo de acesso.

Por exemplo, um empregado da empresa utilizando um equipamento adequadamente configurado e acedendo através da Internet pode adquirir acesso total. O mesmo empregado com um equipamento emprestado e acedendo através da Internet poderá ter apenas acesso ao correio electrónico.

Para adquirir acesso total através da tecnologia SSL VPN requer a instalação de um agente no equipamento remoto. Tipicamente, tal é uma descarga de software realizada no decorrer do processo de ligação e que se extingue no final da sessão. Alguns fabricantes disponibilizam agentes que se mantêm instalados, pelo que na próxima vez que o equipamento tentar aceder à VPN, a descarga do agente é desnecessária.

Na medida em que o SSL é uma tecnologia de nível aplicacional, as políticas podem ser definidas de um modo detalhado para restringir o acesso que o utilizador remoto pretende.

A tecnologia SSL VPN utiliza a porta 443, que a maior parte dos firewalls deixa aberta. Tal torna possível a utilização da tecnologia SSL VPN sem alterar as políticas dos firewalls. ■ CW

VPN SSL - Como assegurar elevados níveis de segurança nas Comunicações

Mário Gomes
Gestão Produto PT Prime

Como aceder à informação nas Organizações em contexto de Mobilidade com garantia de Segurança?

As Organizações actuais necessitam funcionar em estreita ligação com os seus clientes, parceiros de negócio e fornecedores, garantindo o acesso aos sistemas de informação internos a partir de qualquer lugar e em qualquer momento. A emergência do factor mobilidade não se prende, hoje em dia, apenas com a necessidade de estar contactável por telemóvel ou por e-mail. É fulcral poder aceder às aplicações e sistemas internos da Organização, com a mesma rapidez e usufruindo das mesmas permissões e funcionalidades que estão disponíveis no acesso a partir das instalações no local de trabalho. Para além disso, os utilizadores remotos exigem que a forma de acesso aos sistemas internos seja simples, funcional e "user-friendly", reduzindo o seu esforço de utilização e os custos de suporte na operação da solução.

A facilidade no acesso remoto ao Data Center é por isso considerada uma questão importante, sendo esta capacidade de acesso cada vez mais necessária às Organizações para gerirem de forma eficiente os serviços que têm alojados. A possibilidade de aceder remotamente aos sistemas e aplicações centrais da Organização, com garantias de segurança, constitui por si um factor que potencia a utilização dos serviços e sistemas alojados em Data Center por parte de todos os colaboradores em qualquer situação de mobilidade, assegurando assim maior eficiência e eficácia na actividade da Organização. As soluções que permitem aos utilizadores remotos aceder de forma rápida e segura aos serviços disponibilizados em Data Center, sendo baseadas numa arquitectura funcional que possibilita serem facilmente adoptadas e integradas, constituem um factor diferenciador que aumenta a capacidade competitiva das Organizações.

A PT Prime posiciona-se na linha da frente na resposta à implementação de acessos permanentes e remotos às aplicações e serviços disponibilizados a partir do seu Data Center.

Vantagens diferenciadoras do serviço VPN SSL

O serviço de terminação de Túneis VPN SSL permite aceder com elevados níveis de segurança e fiabilidade, a qualquer hora e a partir de qualquer lugar, à infra-estrutura e serviços alojados em Data Center. A solução é baseada no conceito de virtual appliances, que para além de garantir todas as funcionalidades

existentes nas appliances físicas, garante um conjunto de vantagens relevantes, tais como:

Escalabilidade: se as necessidades da Organização vierem a crescer, não será necessário adquirir novo hardware, bastará apenas transportar a solução para outra máquina virtual e adquirir a licença para os novos utilizadores. Estes procedimentos poderão ser concluídos num curtíssimo período de tempo, reduzindo dramaticamente os tempos de provisão;

Aumento do desempenho: o aumento dos recursos (processador, memória, disco) disponíveis para a máquina virtual onde se encontra instalada a solução, pode ser realizado sem necessidade de aquisição de componentes de hardware;

Gestão simplificada: pelo facto da solução estar suportada em máquinas virtuais e ser baseada em interfaces gráficas intuitivas;

Políticas de Segurança: permitem restringir o acesso de cada utilizador remoto a servidores e aplicações específicas, assim como forçar a adopção de medidas de segurança no PC, impedindo o acesso dos terminais não-conformes com a política de segurança da Organização;

Optimização dos custos de investimento: através da utilização dos serviços geridos da PT Prime, ao invés de uma solução dedicada, é possível adoptar um modelo mais vantajoso para a Organização, eliminando a necessidade de efectuar elevados investimentos iniciais.

Para além destas vantagens, o acesso VPN SSL pode ser usado pelos administradores dos servidores e das aplicações alojadas, permitindo uma gestão remota, eficaz e segura, a qualquer hora e a partir de qualquer lugar. Em caso de catástrofe, numa óptica de Business Continuity, o acesso VPN SSL ao Data Center permite o acesso remoto rápido e seguro, fundamental para o restabelecimento da actividade da Organização.

A Segurança como prioridade

O aumento das ligações remotas às infra-estruturas e aplicações das Organizações criam a necessidade de garantir acessos seguros de forma a proteger não só a legitimidade do acesso, como garantir a encriptação da informação a ser transmitida. Face aos cenários de crescente complexidade e mobilidade nas Organizações, é necessário dispor de soluções que assegurem uma ligação segura e permanente às aplicações

empresariais. O serviço de terminação de Túneis VPN SSL garante uma série de funcionalidades imprescindíveis ao acesso seguro dos utilizadores às suas aplicações de rede, tais como: autenticação do utilizador, informação cifrada, disponibilidade permanente no acesso e garantia do acesso poder ser efectuado a partir de qualquer dispositivo móvel. Para tal, o utilizador remoto apenas necessita possuir um terminal, as credenciais exigidas e conectividade à Internet, para poder implementar uma ligação segura às aplicações alojadas em Data Center.

Estes acessos podem ser complementados com soluções de autenticação forte (hardware tokens; software tokens; sms tokens) de forma a elevar ainda mais os níveis de segurança de toda a solução.

Na vanguarda da tecnologia

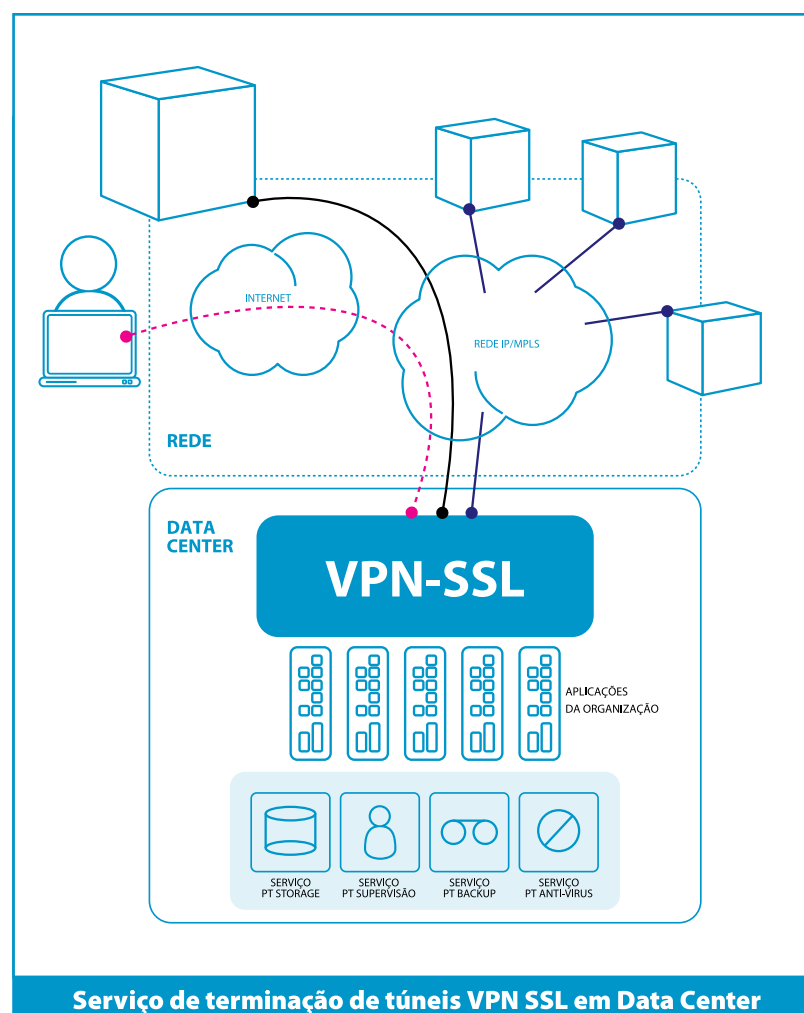
O serviço de terminação de Túneis VPN SSL em Data Center da PT Prime é uma solução que inclui funcionalidades tecnologicamente avançadas:

- Consolidação de acessos VPN SSL numa plataforma unificada best-of-breed de acesso remoto;
- Prevenção de intrusões integrada e protecção de segurança detalhada ao nível do ponto de acesso bloqueando vírus, malware e ataques maliciosos;
- Defesa contra as últimas ameaças com actualizações automáticas e em tempo real, com serviços de IPS integrados.

Para o utilizador final, o serviço VPN SSL maximiza vantagens:

- Garante a segurança da sessão;
- Reforça a segurança quando ligado a partir de computadores públicos ou quiosques de Internet, criando um ambiente de trabalho seguro e fechado;
- Verifica automaticamente a validação da segurança do terminal de acesso antes de efectuar a autenticação, para um nível adicional de segurança;
- Disponível com uma cobertura horária adequada às necessidades da Organização e permite uma interface única para gestão das diversas componentes da sua infra-estrutura.

O serviço VPN SSL da PT Prime possibilita assim às Organizações adquirem funcionalidades avançadas de gestão que permitem a optimização na operação do seu negócio num contexto de complexidade e mobilidade, sem comprometer a segurança dos seus sistemas.



Serviço de terminação de túneis VPN SSL em Data Center

●● PT Prime

www.ptprime.pt