

Acesso remoto corporativo

Visão Geral Historicamente, as organizações têm usado soluções VPN IPSec para fornecer aos funcionários o acesso remoto aos recursos da rede; uma implementação cara e complicada, para apenas uns poucos usuários. Criado originalmente para proteger comunicações entre sites, o IPSec mostrou ser incapaz de acompanhar a crescente demanda por acesso remoto exigida pelas companhias de hoje. Conforme a Internet se torna o método mais importante de distribuição de acesso aos aplicativos de missão crítica pelas companhias e os dispositivos da web, mais difundidos, as limitações das soluções IPSec se mostram proibitivas para muitas empresas. O controlador FirePass da F5 permite às companhias fornecer facilmente um acesso remoto seguro e granular à rede interna e aos aplicativos nela executados, a partir de qualquer dispositivo e em qualquer lugar.

Desafio As organizações que empregam as VPNs enfrentam problemas com o endereçamento IP, tradução de endereços de rede, suporte limitado a dispositivos remotos e a necessidade de instalação de software e manutenção de cada cliente. Como as soluções IPSec exigem software cliente para proteger as transações, os recursos da companhia somente podem ser acessados por intermédio de um número restrito de sistemas. Isso limita muito a capacidade dos usuários finais de obter acesso a recursos importantes a partir de sistemas públicos e dispositivos móveis. Isso também aumenta o custo da implementação, porque exige das companhias que forneçam e mantenham laptops corporativos para cada funcionário em trânsito. Além disso, conforme mais usuários remotos obtêm acesso a informações sigilosas, a integridade e segurança do dispositivo usado se tornou um grande problema de segurança. Como garantir que o sistema esteja protegido e livre de códigos maliciosos?

Os administradores têm de lidar com o amplo controle de segurança desses sistemas VPN IPSec, que não possuem a granularidade necessária para fornecer acesso adequado aos usuários. Os administradores precisam escolher entre um acesso amplo, que compromete a segurança da rede, ou um acesso muito limitado, que dificulta o desempenho de um trabalho eficiente pelos usuários. As soluções VPN IPSec também oferecem auditoria limitada, tornando difícil para os administradores a solução de problemas e o acesso claro aos dados de usuários.

Uma pesquisa realizada pela AT&T/Economist revelou que 54% dos funcionários trabalham em casa regularmente. Estima-se que esse número aumentará para 80% em 2005. As companhias precisam de uma solução que lhes permita fornecer acesso confiável e seguro a múltiplos aplicativos, a partir de vários dispositivos e em qualquer lugar do mundo.

Solução O controlador FirePass® da F5 permite às companhias oferecer acesso remoto seguro, confiável e intuitivo aos aplicativos e dados corporativos, usando tecnologia padrão de navegadores web, sem as dores de cabeça associadas à demorada instalação e configuração de programas no cliente, ou mudanças nos aplicativos do servidor. O dispositivo FirePass também oferece capacidades robustas de proteção da integridade desses clientes, garantindo a conformidade com os padrões da companhia.

O dispositivo FirePass é a primeira solução VPN SSL com suporte completo entre plataformas. Ampliando seu suporte para qualquer aplicativo IP em clientes Apple® Macintosh®, PocketPC e Linux, além do Microsoft® Windows®, e ampliando a segurança de clientes para aplicativos de acesso à web, e-mail e aplicativos de

arquivos, o controlador FirePass oferece a solução mais comum para acesso seguro à rede.

Ele também oferece a única API aberta com SDK que oferece a outros fornecedores de aplicativos a capacidade de implementar o acesso remoto seguro em aplicativos de clientes.

Acesso completo à rede

O usuário de laptops corporativos, ou usuário "confiável", é um funcionário que usa um equipamento fornecido e mantido pela companhia. O usuário confiável é normalmente um executivo ou membro da equipe de vendas que necessita do acesso aos mesmos recursos da rede utilizados pelos usuários no escritório.

Para esses usuários, o controlador FirePass distribui o acesso de rede para sistemas Windows, Macintosh, PocketPC e Linux. As funções padronizadas para todas as plataformas de desktop e laptop incluem a divisão do tráfego em dutos, compactação, limites de tempo baseados em atividade e o lançamento automático de aplicativos.

Para administradores, o dispositivo FirePass permite a restrição e proteção de recursos acessíveis, instituindo regras que limitam o acesso à uma rede ou porta específica. Ele usa o protocolo padrão HTTPS com a SSL como transporte e, isso, portanto, funciona por meio de todos os proxies HTTP, incluindo pontos de acesso público, LANs privadas e redes e ISPs que não suportam as VPNs IPSec tradicionais. Como ele usa a compactação GZIP para compactar o tráfego antes que ele seja criptografado, ele reduz a quantidade de tráfego enviado pela Internet, melhorando o desempenho.

Para proteger contra ataques de backdoor durante o acesso à rede com a divisão do tráfego em dutos, o sistema FirePass oferece um firewall dinâmico que protege os usuários do Windows 2000/XP usando a função de acesso completo à rede. Isso elimina a capacidade de um hacker de rotear, por meio do cliente, para a rede corporativa ou a chance de um usuário enviar tráfego acidentalmente para a rede pública.

O dispositivo FirePass também aumenta a segurança detectando a presença de processos exigidos (antivírus, firewalls pessoais, nível de atualização do SO, configurações do registro e níveis do McAfee® Antivírus) e a ausência de outros processos (como keyloggers, por exemplo) no PC do cliente, antes de permitir o acesso completo à rede. Os usuários que não estiverem em conformidade com essas políticas primárias podem se conectar a uma rede de quarentena, na qual poderão obter as atualizações para atender aos padrões atuais de segurança da companhia.

Acesso ao portal - acesso seguro a partir de sistemas públicos para funcionários, clientes e parceiros

Cada vez mais, as companhias implementam aplicativos baseados na web, portais de intra/extranet e e-mail baseado na web para aumentar a produtividade dos funcionários e a eficiência operacional, tanto interna quanto em relação aos parceiros. Para maximizar os benefícios desses aplicativos, as organizações devem garantir que eles estejam acessíveis aos funcionários e parceiros a partir de qualquer local, garantindo um acesso restrito e seguro, somente para usuários autorizados.

O controlador FirePass oferece várias funções para garantir o acesso seguro baseado na web aos portais intranet e extranet corporativos, webmail e aplicativos. A

capacidade de acesso ao portal funciona em qualquer sistema operacional do cliente com um navegador - Windows, Linux, Macintosh, Pocket PCs, PSAs e mais.

Aplicativos da web

O dispositivo FirePass oferece acesso fácil aos servidores web internos, incluindo o Microsoft Outlook Web Access e o Lotus® Domino Web Acces (antigo iNotes®), como se estivessem na rede interna da companhia. Ele também oferece controle de acesso granular aos recursos da intranet, com base em grupos. Por exemplo, os funcionários podem receber acesso a todos os sites da intranet, enquanto os parceiros são restritos a um host web específico.

Ao acessar recursos, o controlador FirePass mapeia dinamicamente as URLs internas para URLs externas, de forma que não revelem a estrutura interna da rede. Os cookies de usuários são gerenciados no dispositivo FirePass, para evitar a exposição de informações sigilosas. Para os aplicativos que exigem acesso aos cookies, o controlador FirePass pode enviar os cookies para o navegador remoto. As credenciais do usuário podem ser enviadas para os hosts da web para o suporte ao login automático e outros acessos específicos do usuário aos aplicativos. O controlador FirePass também se integra com servidores existentes de gerenciamento de identificação (como o Netegrity®, por exemplo), para habilitar o acesso único aos aplicativos.

Acesso ao servidor de arquivos / E-mail

O controlador FirePass permite aos usuários navegar, copiar, mover, excluir e fazer download ou upload de arquivos em diretórios compartilhados. Ele suporta compartilhamentos SMB, grupos de trabalho do Windows, domínios do NT 4.0 e Windows 2000, Novell 5.1/6.0 com o pacote Native File System e servidores NFS. Para o e-mail, o dispositivo FirePass oferece acesso seguro baseado na web a servidores de mensagens POP/IMAP/SMTP a partir dos navegadores de dispositivos padrão e móveis. Isso permite aos usuários receber e enviar mensagens, anexar arquivos da rede aos e-mails e fazer o download de anexos.

Suporte a dispositivos móveis

O controlador FirePass permite o acesso seguro a partir de PDAs (como o PalmOS) e celulares (WAP e iMode) ao e-mail e outros aplicativos. Ele formata o e-mail dinamicamente a partir dos servidores POP/IMAP/SMTP para que caibam nas telas menores dos PDAs e celulares, e possui suporte ao envio de arquivos da rede como anexos de e-mail, além da visualização de documentos de texto ou do word.

Acesso aos portais - segurança completa

O controlador FirePass oferece múltiplas camadas de controle para proteger o acesso às informações a partir de sistemas públicos. Por exemplo, os usuários do Windows XP/2000 podem ser automaticamente direcionados para um espaço de trabalho protegido durante suas sessões de acesso remoto. No modo de espaço de trabalho protegido, o usuário não pode gravar arquivos fora do espaço protegido, e todas as pastas temporárias e seu conteúdo são excluídas ao fim da sessão. Como a sessão do usuário é em um desktop separado, eles estão protegidos contra cavalos de tróia e keyloggers.

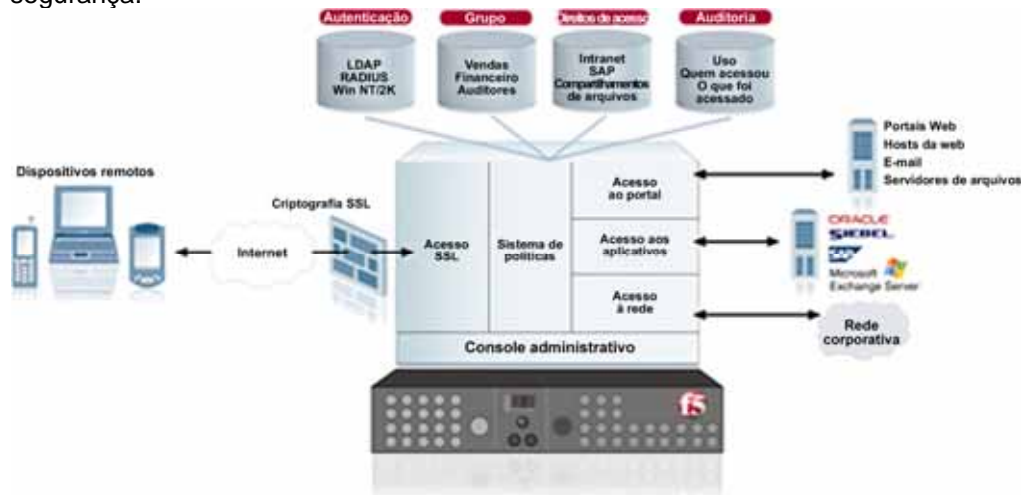
O dispositivo FirePass também possui uma função de controle de limpeza de cache que remove cookies, histórico do navegador, informações do autocompletar, cache do navegador, arquivos temporários e todos os controles ActiveX instalados durante a sessão de acesso remoto a partir do PC cliente. Um "teclado virtual" protegido permite a digitação segura de senhas com o mouse, em vez do teclado. Quando

ativada, essa função permite aos funcionários informar com segurança uma senha a um sistema que foi comprometido por um keylogger.

Para os sistemas que não podem instalar um controle de limpeza, o controlador FirePass pode ser configurado para bloquear o download de todos os arquivos para evitar a possibilidade de esquecer, acidentalmente, arquivos temporários no sistema, mas permitindo o acesso aos aplicativos. Para usuários acessando aplicativos web na rede corporativa, o produto FirePass melhora a segurança dos aplicativos e impede ataques na camada de aplicação (como o cross-site scripting, caracteres inválidos, injeção de SQL e estouro de buffer), fazendo varreduras no acesso aos aplicativos da web e bloqueando o acesso do usuário quando um ataque é detectado. O dispositivo FirePass também é capaz de fazer a varredura de uploads de arquivos e da web, usando um sistema integrado ou externo, por meio da API ICAP. Os arquivos infectados são bloqueados no gateway e não são permitidos nos servidores de e-mail ou arquivos da rede, aumentando a proteção.

Acesso aos aplicativos - acesso seguro a aplicativos específicos

O FirePass permite aos administradores conceder a certos usuários (como parceiros de negócios, usando equipamento não mantido pela companhia) o acesso a sites e aplicativos específicos da extranet. Ele protege os recursos da rede, permitindo somente o acesso aos aplicativos especificamente autorizados pelo administrador do sistema. Os aplicativos suportados incluem servidores de terminal, hosts legados, desktops Windows e sistemas X Windows. O FirePass registra um histórico dos aplicativos específicos acessadas por cada usuário, facilitando as auditorias da segurança.



Acesso aos aplicativos cliente/servidor

O FirePass permite que um aplicativo cliente nativo possa se comunicar com um servidor de aplicativos específico da companhia por meio de uma conexão segura entre o navegador e o controlador FirePass. Isso não exige que o usuário instale ou configure qualquer programa. No lado da rede, o FirePass não exige qualquer programa adicional nos servidores de aplicativos acessados. Ele usa o protocolo padrão HTTPS com a SSL como transporte, funcionando por meio de de todos os proxies HTTP, incluindo pontos de acesso público, LANs privadas e redes e ISPs que não suportam as VPNs IPsec tradicionais. Os aplicativos suportados incluem o Outlook para Clusters Exchange, FTP passivo, Citrix Nfuse e o mapeamento de unidades de rede. Para um melhor desempenho, a compactação também é suportada.

Acesso ao servidor de terminal

O FirePass fornece acesso seguro, baseado na web, aos servidores de terminal Microsoft, aplicativos MetaFrame® da Citrix®, áreas de trabalho remotas do Windows XP e servidores VNC. Ele suporta opções de grupos de acesso, autenticação de usuários e funções de logon automático para usuários autorizados, bem como o download e a instalação automáticos do componente cliente correto dos serviços de terminal ou plataforma remota Citrix, caso não esteja atualmente instalado no dispositivo remoto.

Acesso ao Host

Essa função permite ao FirePass proteger o acesso baseado na web dos aplicativos legados VT100, VT320, Telnet, X-Term e IBM 3270/5250, sem precisar de modificações nos aplicativos ou servidores, a partir de navegadores web com suporte ao Java ou controles ActiveX.

Acesso ao Desktop

Combinando as funções do controlador FirePass às funções existentes de acesso à área de trabalho remota integradas no Windows XP ou por meio de funcionalidades que podem ser acionadas com o uso de programas gratuitos e disponíveis para praticamente qualquer sistema operacional de desktops, o FirePass pode oferecer um acesso transparente a qualquer ambiente desktop, a partir de navegadores web com suporte ao Java ou controles ActiveX.

Autenticação e autorização

O controlador FirePass oferece um editor visual de políticas (Visual Policy Editor - VPE) que permite à companhia determinar os requisitos para o cliente, antes mesmo que ele possa fazer o login. O VPE oferece um processo autodocumentado e fácil de entender a fim de definir e divulgar a política da companhia, e providencia a solução para usuários, caso um cliente não esteja em conformidade com tal política. Isso permite à companhia não somente impedir a conexão de sistemas que poderiam prejudicar a rede, mas também documentar esse processo e fornecer um meio para que os usuários façam o próprio reparo sozinhos, sem a necessidade de suporte.

O controlador FirePass também inclui um sistema dinâmico de políticas, permitindo aos administradores gerenciar facilmente a autenticação de usuários e a autorização de privilégios. O acesso baseado em políticas dinâmicas dá aos administradores um controle rápido e granular sobre os recursos da rede. Com o apoio das regras, os administradores podem autorizar o acesso aos aplicativos com base no usuário e no dispositivo sendo usado (de acordo com o resultado da verificação anterior ao logon). Por exemplo, os administradores podem configurar as permissões de um usuário para permitir acesso somente ao e-mail a partir de um quiosque público, como limpeza ativa de arquivos temporários e cache, mas oferecendo o acesso completo à rede a partir de um laptop corporativo com firewall e programa antivírus ativos.

Por padrão, os usuários são autenticados em uma base de dados interna do FirePass, usando senhas. Porém, o dispositivo FirePass pode ser facilmente configurado para trabalhar com os métodos de autenticação RADIUS, LDAP e Active Directory (Kerberos), autenticação HTTP básica e mediante formulário, servidores de gerenciamento de identidade (como o Netegrity) e servidores de domínio Windows. Muitas companhias exigem uma autenticação de fator duplo, que usa métodos além do nome de usuário e senha. O FirePass possui suporte completo aos sistemas de autenticação RSA SecurID® e VASCO Digipass®, baseados em tokens.



Além disso, o controlador FirePass permite ao administrador restringir ou liberar o acesso com base no dispositivo usado para acessar o FirePass. O controlador FirePass também pode verificar a presença de certificados digitais do cliente durante o login do usuário. Esse certificado somente estará presente no laptop. Com base na presença desse certificado digital, o dispositivo FirePass pode suportar o acesso a uma gama maior de aplicativos. O controlador FirePass também pode usar o certificado do cliente como uma forma de autenticação de fator duplo, proibindo qualquer acesso à rede para os usuários sem um certificado de cliente válido. O dispositivo FirePass pode agir como autoridade certificadora e gerar e distribuir automaticamente os certificados de clientes. Isso reduz drasticamente os custos adicionais de aquisição e gerenciamento de certificados para cada um dos clientes.

Integridade do cliente

O controlador FirePass inclui um conjunto de componentes para oferecer a verificação da integridade de clientes remotos, antes mesmo de permitir o login. A checagem de integridade permite às companhias verificar se o dispositivo remoto atende aos padrões definidos. Em sistemas Windows, por exemplo, o FirePass suporta os fornecedores de 16+ antivírus e 7+ firewalls pessoais, dando à companhia a flexibilidade para definir a necessidade desses aplicativos, sem exigir fornecedores específicos e sem a necessidade de adquirir e instalar um novo produto. Além disso, o VPE permite às companhias verificar arquivos, processos, os certificados de clientes, IP de origem, nível de atualização, características do SSL, sistema operacional, etc. Essas informações podem ser usadas para restringir o acesso de um usuário a sistemas específicos, ou mesmo impedi-lo de fazer o login.

Privilégios de acesso

Os privilégios de acesso podem ser concedidos a indivíduos ou a grupos de usuários (por exemplo, "Vendas", "Parceiros", "TI"). Isso permite que o dispositivo FirePass restrinja os grupos e indivíduos a certos recursos. Os parceiros podem receber acesso somente a um servidor extranet, enquanto a equipe de vendas pode se conectar ao e-mail, à Intranet da companhia e ao sistema CRM. As políticas de acesso podem ser definidas para grupos de recursos, em vez de recursos individuais. Outros recursos podem ser simplesmente adicionados a um grupo de recursos, sem modificar manualmente as políticas de acesso individuais. Além disso, os recursos podem ser definidos como uma máscara, fazendo que quaisquer mudanças nas definições de recursos sejam automaticamente atualizadas em todo as máscaras. Essas capacidades reduzem de maneira significativa a complexidade do gerenciamento de políticas em ambientes corporativos com um grande número de grupos de usuários e recursos.

O controlador FirePass também oferece flexibilidade às companhias, fornecendo funções administrativas (registro de novos usuários, encerramento de sessões, redefinição de senhas) para alguns usuários-administradores, sem expor todas as funções a eles (por exemplo, desligar um servidor, excluir um certificado). Mais ainda, as autoridades podem ser restritas a grupos específicos de usuários: um administrador do grupo financeiro, por exemplo, não poderia excluir um usuário do grupo vendas.

Auditoria

O dispositivo FirePass oferece relatórios dos registros da sessão e de ativação. Relatórios resumidos agregam o uso por dia da semana, hora do dia, sistema operacional usado para o acesso, funções usadas, sites da web visitados, duração da sessão, tipo de encerramento da sessão e outras informações em um intervalo de tempo específico para um usuário.



API iControl para clientes VPN SSL - acesso seguro aos aplicativos

Sendo o único produto VPN SSL com uma API e SDK abertos, o controlador FirePass permite o acesso automatizado e seguro para os aplicativos clientes Win32, fornecendo comunicação segura sistema-a-sistema ou aplicativo-a-aplicativo. Agora, os aplicativos podem iniciar e encerrar automaticamente as conexões de rede, de forma transparente, sem exigir dos usuários que efetuem o login na VPN. Isso permite conexões mais fáceis e rápidas para usuários finais, reduzindo a instalação de aplicativos clientes.