



Principais Benefícios:

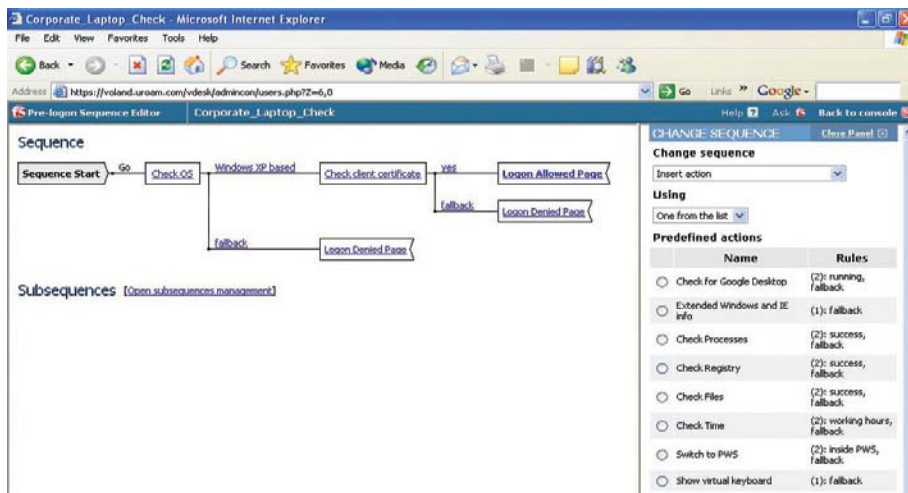
- Maior produtividade de funcionários remotos e móveis – trabalhe a partir de qualquer lugar
- Elevado Retorno de Investimento – fornece uma plataforma comum a todas as necessidades de acesso remoto seguro
- Menos custos com suporte
- Política granular de segurança – minimize os riscos do negócio

Melhor VPN em SSL do Mercado

O appliance FirePass® SSL VPN da F5 fornece acesso seguro às aplicações e dados corporativos, seja através de um navegador web padrão e ou de um cliente independente. O FirePass também oferece um excelente desempenho, escalonabilidade, facilidade de uso e segurança nos terminais para garantir a produtividade daqueles que trabalham em casa ou em trânsito, sem comprometer a segurança dos dados e aplicações corporativas.

Principais Benefícios:

- **Gerenciamento de Política Extraordinário** – O exclusivo Visual Policy Editor oferece, além da redução dos custos de gerenciamento, uma interface apont-e-clique, fácil e intuitiva para gerenciamento detalhado da política de acesso.
- **Segurança Integrada de Terminal** – Oferece um ambiente de trabalho virtual seguro, com verificações da integridade do terminal antes do login e gerenciamento da confiabilidade de terminal para uma administração tranquila e com menos aborrecimentos administrativos.
- **Mais Amplo Suporte de Aplicação** – Oferece um acesso seguro e fácil ao e-mail, portais da web, serviços de arquivo de rede, serviços de terminal, CRM e outras aplicações empresariais fundamentais nos dispositivos cliente gerenciados e não-gerenciados a partir de qualquer local.
- **Amplo Suporte ao Cliente** – O FirePass oferece um amplo suporte multiplataforma, para um acesso seguro à rede a partir de Windows (2000, ME, XP, Vista), Mac, Linux e Windows Mobile 5 e 6, Pocket PC e telefone inteligente.
- **Escalonabilidade e Desempenho de Classe Corporativa** – Suporta até 2.000 sessões concomitantes em um dispositivo único e fácil de gerenciar. Até 10.000 diferentes sessões concomitantes podem ser suportadas pela integração com o BIG-IP Local Traffic Manager da F5. Otimiza a experiência do usuário final, usando recursos como a compactação de qualquer tráfego de IP da aplicação e o cache no lado servidor para aplicações web.
- **Ampla Interoperabilidade** – Suporta a infra-estrutura de rede existente e o sistema de gerenciamento de identidade por Active Directory, Radius, LDAP, PKI, RSA, ACE e outros. Oferece integração de portal web com suporte para applets em Java, programação em JavaScript e outros (certificado VPNC).
- **Líder no Setor em Alta Disponibilidade Global** – A exclusiva integração com o BIG-IP Global Traffic Manager da F5 fornece uma alta disponibilidade por toda a WAN no caso de desastres no local. O suporte de redirecionamento também oferece alta disponibilidade dentro do local..



O exclusivo Visual Policy Editor permite criar um fluxograma gráfico das suas políticas de acesso – facilitado a criação e o gerenciamento de grupos, usuários, dispositivos ou qualquer combinação dos três com o recurso simples de apontar-e-clicar. Isso simplifica a definição e o gerenciamento de políticas de terminais, reduz custos administrativos e garante que a proteção dos recursos da empresa seja assegurada com rapidez.



Acesso à Rede



Acesso à Rede FirePass para os sistemas Windows (Vista, XP, 2000), Mac e Linux:

- O Windows Installer Service elimina a necessidade de privilégios administrativos especiais nas atualizações de componente dos clientes FirePass, reduzindo os custos de gerenciamento.
- Fornece um acesso remoto seguro à rede para todas as aplicações baseadas em IP (TCP, UDP).
- Entre as funções padrões para todas as plataformas desktop e laptop incluem-se "split tunneling", compactação, limites de tempo por inatividade e execução automática de aplicações.
- Diferentemente das VPNs em IPSec, fornece um acesso remoto sem exigir a instalação de programas no cliente nem a configuração do dispositivo remoto. Não é necessária qualquer mudança na aplicação seja lado servidor ou cliente.
- Permite aos administradores restringir e proteger os recursos acessíveis por meio do conector através de regras que limitam o acesso a uma rede ou porta específica.
- Usa o protocolo padrão HTTPS com SSL como transporte, o que, portanto, funciona em todos os proxies HTTP, incluindo pontos de acesso público, LANs privadas e através das redes e dos ISPs que não suportam as tradicionais VPNs em IPSec.
- Antes que o tráfego seja criptografado, utiliza a compactação GZIP, reduzindo a quantidade de tráfego enviada pela Internet, o que melhora o desempenho.

Segurança do Cliente

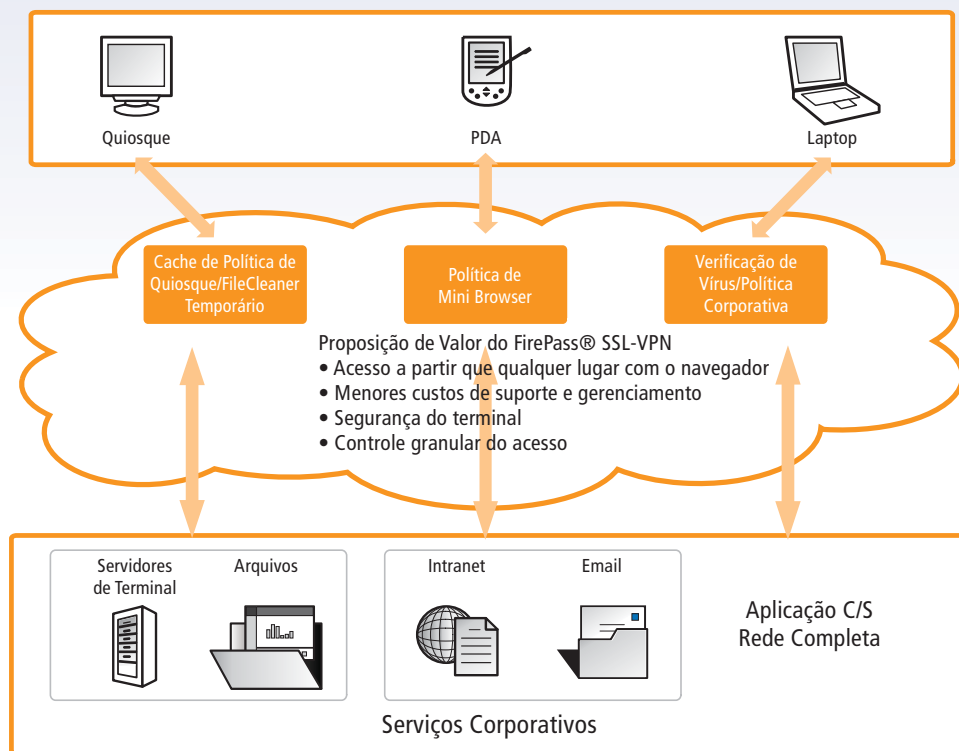
- Split tunneling Seguro – Contra ataques de backdoor durante o uso da rede com split tunneling, o sistema FirePass oferece um firewall dinâmico que protege os usuários do Windows 2000/XP usando a função complete network access. Isso elimina a possibilidade de um hacker entrar, por meio do cliente, na rede corporativa ou a chance de um usuário enviar acidentalmente o tráfego para a rede pública.
- Verificação da Integridade do Cliente – O FirePass também aumenta a segurança, detectando no PC do cliente a presença de processos fundamentais (como antivírus, firewalls pessoais, nível da atualização do SO, configurações do registro, etc.) e a ausência de outros processos (como keyloggers, por exemplo), antes de permitir o acesso completo à rede.

Recursos do Windows Network Access

- Cliente Windows Independentes – O Firepass estabelece uma conexão de rede após registrar as credenciais do usuário. O programa pode ser distribuído automaticamente ao cliente usando a tecnologia MSI Installer da Microsoft.
- Integração com o Logon/GINA do Windows – Permite um logon transparente, implícito, de usuários à rede corporativa, pela integração com o processo de logon GINA (notificação do "ctrl + alt + del")
- CLI Cliente de VPN Independente – A interface de linha de comando (CLI) suporta a conexão individual por meio da integração com aplicações de terceiros (como programa de discador remoto).
- Discador de VPN do Windows – Fornece uma experiência simplificada para os usuários finais que se sentem mais confortáveis com a interface discada.
- Oferece o Mapeamento Automático de Unidade – As unidades da rede podem ser mapeadas automaticamente para um usuário do Windows.
- Oferece Suporte a IP Estático – Define um IP estático baseado no usuário quando estabelecido um acesso à rede por conexão VPN – reduzindo os custos de suporte administrativo.
- Acesso Transparente à Rede - Elimina as janelas pop-ups do navegador de acesso à rede; previne que os usuários finalizem a conexão acidentalmente.

Suporte a Dispositivos Móveis

- Acesso seguro às aplicações a partir do Windows Mobile 5 & 6, do PocketPC e de telefones inteligentes.
- Acesso tanto às aplicações web quanto às aplicações cliente/ servidor.



Acesso aos aplicativos - Acesso Seguro a Aplicações Específicas

O FirePass permite aos administradores conceder a certos usuários (como parceiros de negócios que usam equipamento não mantido pela empresa) o acesso a sites e aplicações específicas da extranet. O FirePass protege os recursos da rede, permitindo somente o acesso às aplicações especificamente autorizadas pelo administrador do sistema.

Acesso às Aplicações Cliente/Servidor

- Permite que uma aplicação nativa do lado cliente possa se comunicar com um servidor de aplicação específico da empresa por meio de uma conexão segura entre o navegador e o controlador FirePass.
- Isso não exige que o usuário instale previamente ou configure qualquer programa.
- No lado da rede, o FirePass não exige qualquer programa adicional nos servidores de aplicação acessados.
- Usa o protocolo padrão HTTPS com SSL como transporte e, portanto, funciona em todos os proxies HTTP, incluindo pontos de acesso público, LANs privadas, e em redes e ISPs que não suportam as tradicionais VPNs por IPSec.
- Entre as aplicações suportadas incluem-se o Outlook para Clusters Exchange, FTP passivo, Citrix Nfuse e o mapeamento de unidades de rede.
- Os administradores também podem permitir o suporte às aplicações personalizadas, inclusive CRM e outras que utilizam portas TCP estáticas.
- Suporta o autologin a aplicações AppTunnels, Citrix e WTS para simplificar a experiência do usuário.
- Suporta a execução automática das aplicações no lado cliente para simplificar a experiência do usuário final e reduzir os custos de suporte.
- Suporte exclusivo para compactação do tráfego das aplicações cliente/servidor na WAN, para um melhor desempenho.

Acesso ao Terminal Server

- Fornece acesso seguro, baseado na web, a servidores de terminal Microsoft, aplicações MetaFrame® da Citrix®, áreas de trabalho remotas do Windows XP e servidores VNC.
- Suporta opções de acesso de grupo, autenticação de usuário ou logon automático de usuários autorizados.
- Suporta download automático e instalação correta dos serviços terminal ou do componente de cliente da plataforma remota Citrix, caso não esteja atualmente instalado no dispositivo remoto, poupando tempo.
- Suporta o acesso remoto a áreas de trabalho do XP para solução a distância de problemas, usando RDP ou áreas de trabalho que não sejam do XP, utilizando a função VNC embutida.

AppTunnels Dinâmicos

- Oferece suporte máximo ao acesso a grande variedade de aplicações cliente/servidor e aplicações web.
- Proporciona a melhor alternativa aos proxies reversos para o acesso de aplicações em dispositivos de clientes Windows.
- Elimina a necessidade do teste de interoperabilidade de conteúdo de aplicação web.
- Exige apenas os privilégios de "usuário avançado" na instalação, e nenhum privilégio especial na execução.
- Fornece suporte adicional para abertura automática dos túneis de aplicação web, simplificando a experiência do usuário final.

Acesso ao Host

- Permite um acesso seguro através da web às aplicações VT100, VT320, Telnet, X-Term e IBM 3270/5250 ainda em uso.
- Não requer nenhuma modificação nas aplicações nem nos servidores de aplicação.
- Elimina a necessidade de programa de terceiros para acesso ao host, reduzindo o TCO (Total Cost of Ownership).



Portal Access—Acesso por Proxy a Aplicações Web, Arquivos e E-mail.

O recurso FirePass Portal Access funciona em qualquer sistema operacional cliente que tenha um navegador – Windows, Linux, Macintosh, Pocket PCs, PDAs e outros.

O Portal Access Disponível no FirePass:

Aplicações Web

- Fornece acesso aos servidores web internos, inclusive Microsoft Outlook Web Access, Lotus iNotes e MS SharePoint Portal, tão fácil quanto se esse fosse dentro da LAN corporativa.
- Oferece, com base em grupos, controle de acesso granular aos recursos da intranet. Por exemplo, os funcionários podem receber acesso a todos os sites da intranet, enquanto os parceiros permanecem restritos a um host web específico.
- Ao acessar recursos, o FirePass mapeia dinamicamente os endereços internos para endereços externos, de forma que não revelem a estrutura interna da rede.
- Os cookies de usuários são gerenciados no FirePass Controller, para evitar a exposição de informações sigilosas.
- As credenciais do usuário podem ser enviadas para os hosts web dando suporte ao login automático e a outros acessos específicos de usuário aos aplicativos. O FirePass também se integra com servidores existentes de gerenciamento de identificação (como o Netegrity®, por exemplo), para permitir o acesso único às aplicações.
- O FirePass intermedia as requisições de login dos hosts web, evitando que usuários mantenham suas senhas no cache dos navegadores cliente.
- Lista de Controle de Acesso Granular (ACL) – Permite ou restringe o acesso a partes específicas de uma aplicação, para maior segurança e menores riscos ao negócio.
- Fornece suporte à split tunneling para aplicações web, resultando em um desempenho mais rápido dos usuários que acessam sites públicos.
- Cache dinâmico no lado servidor, para melhorar o desempenho das aplicações web (proxy reverso) e acelerar os downloads de páginas.
- Oferece suporte de fábrica ao proxy reverso para reescrever uma grande quantidade de conteúdo em JavaScript na páginas da web, poupando tempo.

Acesso ao Servidor de Arquivos

- Permite aos usuários navegar, copiar, mover, excluir e fazer download ou upload de arquivos em diretórios compartilhados.
- 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.

Acesso ao E-mail

- Fornece um acesso seguro, baseado em web, para servidores de e-mail POP/IMAP/SMTP de navegadores móvel e padrão.
- Permite aos usuários receber e enviar mensagens, anexar arquivos da rede aos e-mails e fazer o download de anexos.

Suporte a Dispositivos Móveis

- Acesso seguro de PDAs, PocketPCs, telefones inteligentes, celulares, iPhones, WAP e iMode para e-mail e outras aplicações baseadas em web.
- 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.
- Suporta ActiveSync – O suporte à aplicação ActiveSync permite, a partir de um dispositivo PDA, a sincronização de e-mail e calendário com o Exchange Server sem a necessidade do cliente VPN pré-instalado.

Portal Access – Segurança Abrangente

O FirePass oferece múltiplas camadas de controle para proteger o acesso às informações a partir de sistemas públicos.

Segurança do Cliente

- Ambiente de Trabalho Protegido - 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 desse espaço, e todas as pastas temporárias e seu conteúdo são excluídas ao fim da sessão.
- Limpeza de Cache – O controle de limpeza de cache, além de esvaziar a lixeira, remove os seguintes dados do PC do cliente: cookies, histórico do navegador, informações da função autocompletar, cache do navegador, arquivos temporários, todos os controles ActiveX instalados durante sessão de acesso remoto.
- Teclado Virtual Seguro - Para uma segurança adicional das senhas, o FirePass oferece um Teclado Virtual Seguro (licença pendente) que permite digitar senhas usando o mouse, em vez do teclado.
- Bloqueio de Downloads – Para os sistemas que não podem instalar um controle de limpeza, o FirePass pode ser configurado para bloquear o download de todos os arquivos, evitando a possibilidade de esquecer, acidentalmente, arquivos temporários no sistema, mas permitindo o acesso aos aplicativos.

Inspeção de Conteúdo e Segurança de Aplicação de Web

Para usuários que acessam a rede corporativa, o FirePass aumenta a segurança das aplicações 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 às aplicações web e até mesmo bloqueando os usuários quando um ataque é detectado.

Proteção Integrada de Vírus

Por meio da API ICAP, o FirePass é capaz de fazer a varredura de uploads de arquivos e da web, usando um sistema integrado ou externo. Os arquivos infectados são bloqueados no gateway e não são permitidos nos servidores de e-mail ou arquivos da rede, aumentando a proteção.



Policy Engine Dinâmico – Controle Administrativo Total

O FirePass Policy Engine é um mecanismo de política que permite aos administradores gerenciar com facilidade os privilégios de autorização e as autenticações dos usuários.

Acesso Dinâmico Baseado em Políticas

Com o FirePass, os administradores têm um controle rápido e granular sobre os recursos da rede. Por meio de políticas, os administradores podem autorizar o acesso às aplicações de acordo com o usuário e o dispositivo usado.

Autenticação de Usuário

Por padrão, os usuários são autenticados em uma base de dados interna do FirePass, usando senhas. Porém, o FirePass pode ser facilmente configurado para trabalhar com os métodos de autenticação RADIUS, LDAP e Active Directory, autenticação HTTP básica e mediante formulário, servidores de gerenciamento de identidade (como o Netegrity) e servidores de domínio Windows.

Autenticação de Fator Duplo

Muitas empresas exigem uma autenticação de “fator duplo”, a qual usa métodos além da identificação e senha de usuário. O FirePass suporta autenticações de fator duplo, incluindo RSA SecurID® Native ACE.

Suporte a PKI/Certificado no Lado Cliente

O FirePass permite ao administrador restringir ou liberar, com base no dispositivo usado, o acesso ao FirePass Controller. O FirePass também pode verificar a presença de certificados digitais no lado cliente durante o login do usuário. Com base na presença desse certificado digital, o FirePass pode suportar o acesso a uma gama maior de aplicações. O controlador FirePass também pode usar o certificado no lado cliente como uma forma de autenticação de fator duplo, proibindo qualquer acesso à rede dos usuários sem um certificado válido no cliente.

Gerenciamento de Grupo

Os privilégios de acesso podem ser concedidos a indivíduos ou a grupos de usuários (por exemplo: “Vendas”, “Parceiros”, “TI”). Isso permite que o FirePass restrinja alguns recursos a certos grupos e indivíduos.

Mapeamento Dinâmico de Grupo

O FirePass mapeia os usuários dinamicamente nos grupos, usando vários mecanismos de mapeamento dinâmico, como o Active Directory, RADIUS, LDAP, Certificados Cliente, Landing URI, nome de Host Virtual e também Sessões Variáveis de pré-logon.

Limites de Tempo de Sessão

Os administradores podem configurar os limites de tempo de inatividade da sessão para proteção contra tentativas de hackers de roubar a sessão de um usuário que se esqueceu de encerrar a conexão em um quiosque.

Administração Baseada em Papéis

O FirePass oferece flexibilidade às empresas, fornecendo funções administrativas (como 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).

Relatório & Registro

O FirePass oferece suporte integrado ao registro dos eventos de usuário, administrador, sessão, aplicação e sistema. Além disso, o FirePass fornece registros no formato silo para integração com um servidor syslog externo. A console de administração proporciona uma ampla gama de relatórios para ajudar a cumprir as auditorias de segurança. Relatórios resumidos totalizam 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 especificado pelo usuário.

Personalização

Interface do Usuário Regionalizada

O FirePass permite que todos os campos na página da web do usuário final sejam regionalizados, incluindo os nomes dos recursos (ex., aplicações web). Isso permite que as empresas regionalizem a interface do usuário final e não apenas seus favoritos – facilitando o uso.

Completa Personalização do Login e WebTop

Com o FirePass, os administradores podem personalizar completamente um login inteiro e uma página webtop para melhor se adaptar aos portais web corporativos existentes. O FirePass permite, para uma melhor experiência do usuário, o upload de páginas personalizadas usando as capacidades WebDAV.

API Cliente iControl SSL VPN - Acesso Seguro Para Aplicativos

Sendo o único produto de VPN em SSL com API e SDK abertos, o FirePass permite o acesso automatizado e seguro para sistemas operacionais clientes Win32 (2000, XP e Vista), fornecendo comunicação protegida sistema-a-sistema ou aplicação-a-aplicação. Agora, os aplicativos podem iniciar e encerrar automaticamente as conexões de rede, de forma transparente, sem exigir que os usuários efetuem o login na VPN. Isso permite conexões mais fáceis e rápidas para usuários finais, reduzindo o custo de instalação da aplicação cliente.



FirePass Série 1200



FirePass Série 4100 & 4300



Detalhes do Produto

A série de appliances do FirePass apresenta três modelos para suprir as necessidades do acesso concomitante dos usuários de pequenas a grandes empresas.

FirePass Série 1200

O appliance FirePass 1200 foi projetado para empresas de pequeno ou médio porte e filiais, e suporta de 10 a 100 usuários concomitantes.

FirePass Série 4100

O controlador FirePass 4100 foi projetado para empresas de médio porte, sendo recomendado, pelo custo-benefício, para até 500 Usuários Concomitantes (O FirePass 4100 pode suportar até 2.000 usuários concomitantes).

FirePass Série 4300

O appliance FirePass 4300 foi projetado para empresas de médio ou grande porte e serviços de provedor, e pode suportar até 2.000 usuários concomitantes.

Clustering

Ambas as aplicações do FirePass 4100 e 4300 suportam clustering e até 10 aplicações que podem ser agrupadas com balanceamento de carga, usando os dispositivos F5 BIG-IP GTM e LTM para oferecer escalabilidade, desempenho e disponibilidade líderes de mercado.

Redirecionamento em Caso de Falha

Os appliances FirePass também podem ser configurados para redirecionar entre pares de servidores (um servidor ativo e outro em prontidão), com a finalidade de evitar que os usuários tenham, em uma improvável falha da unidade, que fazer login novamente a outro FirePass.

Opção de Aceleração de SSL por Hardware

O FirePass 4100 oferece uma opção exclusiva de hardware para Aceleração de SSL para reduzir tanto a carga com a troca de chave como o tráfego de codificação e decodificação SSL. Isso permite, em ambientes de grandes empresas, um ganho de desempenho significativo na codificações com processamento intensivo como o 3DES e AES.

Opção de Aceleração de SSL em FIPS por Hardware*

O FirePass é compatível com o FIPS e está em conformidade com as fortes exigências de segurança das organizações governamentais, de saúde, finanças e outras organizações preocupadas com a segurança. O FirePass 4100 e o 4300 oferecem suporte a armazenamento à prova de falsificação de chaves SSL no nível 2 do FIPS 140, assim como suporte com código certificado FIPS para codificação e decodificação de tráfego SSL por hardware. O Acelerador SSL FIPS está disponível, como opção de fábrica, para instalação nas plataformas 4100 e 4300.

* O FIPS 140-2 atende aos critérios de segurança da CESG (Autoridade Técnica Nacional do Reino Unido para Segurança de Informação) para uso do tráfego privado de dados.

Especificações de Hardware

FirePass 1200

Suprimento de Energia:

Fonte única de 250 W reais

Peso: 4,5 kg.

Dimensões: Chassis para Rack Padrão 1.7"A x 16.7" L x 11" D1U

Aprovação dos Órgãos de Segurança:

UL 60950 (UL 1950-3) CSA-C22.2

No. 60950-00 (Padrão Binacional com UL

60950) CERTIFICAÇÃO DE TESTE CB

PARA IEC 950 EN 60950

Temperatura (operação):

41°F a 104°F (5°C a 40°C)

Umidade (relativa):

20% a 90% a 40°C

FirePass 4100

Suprimento de Energia:

Fonte de 400 W 90/240 +/- 10% VAC bi-volt.

Fonte redundante opcional

Peso: 18 kg.

Dimensões: Chassis para Rack Padrão

3,5"A x 17,5" L x 23,5" D2U

Aprovação dos Órgãos de Segurança:

UL 60950 (UL 1950-3) CSA-C22.2

No. 60950-00 (Padrão Binacional com UL

60950) CERTIFICAÇÃO DE TESTE CB

PARA IEC 950 EN 60950

Temperatura (operação):

41°F a 104°F (5°C a 40°C)

Umidade (relativa):

20% a 90% a 40°C

FirePass 4300

Suprimento de Energia:

Duas fontes de 460 W 90/240 +/- 10% VAC bi-volt

Peso: 19,5 kg.

Dimensões: Chassis para Rack Padrão

3,5"A x 17,5" L x 23,5" D2U

Aprovação dos Órgãos de Segurança:

UL 60950 (UL 1950-3) CSA-C22.2

No. 60950-00 (Padrão Binacional com UL

60950CB) CERTIFICAÇÃO DE TESTE PARA

IEC 950 EN 60950

Temperatura (operação):

41°F a 104°F (5°C a 40°C)

Umidade (relativa):

20% a 90% a 40°C



F5 Networks, Inc.
Sede Corporativa

401 Elliott Avenue West
Seattle, WA 98119
(206) 272-5555 Voice
(888) 88BIGIP Toll-free
(206) 272-5556 Fax
www.f5.com
info@f5.com

F5 Networks
Ásia-Pacífico

+65-6533-6103 Voice
+65-6533-6106 Fax
info.asia@f5.com

F5 Networks Ltd.
Europa/Oriente Médio/África

+44 (0) 1932 582 000 Voice
+44 (0) 1932 582 001 Fax
emeinfo@f5.com

F5 Networks
Japão K.K.

+81-3-5114-3200 Voice
+81-3-5114-3201 Fax
info@f5networks.co.jp