

FirePass – L'accès distant sécurisé



CONNECTEUR VPN - L'ACCÈS SÉCURISÉ POUR LES UTILISATEURS D'ORDINATEURS PORTABLES DE L'ENTREPRISE

L'utilisateur d'ordinateur portable d'entreprise est un employé utilisant un équipement fourni et maintenu par la société. Cet utilisateur est généralement un cadre ou un membre de l'équipe commerciale qui nécessite le même type d'accès aux ressources du réseau que les utilisateurs sédentaires du bureau.

Le connecteur VPN FirePass

- Assure un accès distant sécurisé à la totalité du réseau pour toutes les applications basées sur IP (TCP,UDP).
- Contrairement aux VPN IPSec traditionnels, permet l'accès distant sans requérir l'installation d'un logiciel client et la configuration du dispositif distant. Aucune modification n'est nécessaire aux applications, ni côté client, ni côté serveur.
- Permet aux administrateurs de restreindre et de protéger des ressources à travers le connecteur en instituant des règles limitant l'accès à un réseau ou port spécifique.
- Peut être configuré pour refuser l'accès aux utilisateurs ne disposant pas des bonnes accréditations, tout en donnant aux utilisateurs autorisés l'accès aux ressources dont ils ont besoin. Les mises à niveau et remplacements des PC n'impliquent aucun supplément de travail pour la maintenance du VPN. Les modifications apportées au réseau, mots de passe utilisateurs ou aux adresses IP sont propagées automatiquement vers le PC de l'utilisateur.
- Permet aux administrateurs de détecter les antivirus et firewalls individuels sur les PC clients.
- Utilise la compression GZIP pour réduire le trafic avant qu'il ne soit chiffré, réduisant ainsi le volume échangé sur Internet - et améliorant ainsi les performances
- Disponibilité sans interruption - Dans les configurations comptant un FirePass actif et un autre redondant en attente sur le réseau, l'utilisateur sera transféré sans interruption de service vers le serveur de back up en cas de problème justifiant la bascule.
- Assure le mapping automatique des unités - en cas d'activation du connecteur VPN, les unités réseau peuvent être automatiquement mappés sur le PC de l'utilisateur.

INFORMATIONS COMMERCIALES

Le logiciel FirePass est disponible sur deux types de systèmes dédiés :



Gamme FirePass 1000

Le contrôleur FirePass 1000 est un serveur rackable au format 1U conçu pour les petites et moyennes entreprises. Il supporte 100 utilisateurs simultanés et constitue une solution complète pour l'accès distant, via le Web, aux applications et postes de travail de l'entreprise. Le serveur FirePass 1000 supporte l'ensemble de la gamme des logiciels FirePass.



Gamme FirePass 4000

Le contrôleur FirePass 4000 est un serveur rackable au format 2U conçu pour les grandes entreprises. Il supporte 1000 utilisateurs simultanés et constitue une solution complète pour l'accès distant, via le Web, aux applications et postes de travail de l'entreprise. Le serveur FirePass 4000 supporte l'ensemble de la gamme des logiciels FirePass.

Haute disponibilité

Les contrôleurs FirePass peuvent être associés par paire et configurés pour basculer à chaud sur l'autre serveur de la paire (un serveur actif et un en stand-by), sans que la session ne soit interrompue ou terminée. Ainsi, dans le cas peu probable d'une panne du serveur, toutes les données d'une session sont préservées et la bascule vers l'unité de back up est transparente pour l'utilisateur.

Mise en clusters

Les contrôleurs FirePass 4000 peuvent être associés en clusters pour supporter jusqu'à 10.000 connexions simultanées sur une seule URL logique, sans dégradation des performances. Des fonctions d'équilibrage de charge de pointe permettent de distribuer les sessions entre les différents serveurs disponibles pour maximiser le débit.



F5 Networks SARL
Le Sésame
8, rue Germain Soufflot
78190 Montigny-le Bretonneux
France
Tel: +33 (0) 1 39 30 38 90
Fax: +33 (0) 1 39 30 38 91

F5 Networks Ltd
EMEA Headquarters
Clarke House
65 High Street
Egham
Surrey TW20 9EY
UK
Tel: +44 (0) 800 587 2233
Fax: +44 (0) 1784 497211



CONTROL YOUR WORLD

© 2003 F5 Networks, Inc. Tous droits réservés. BIG-IP, 3-DNS, FirePass et F5 sont des marques commerciales ou des marques déposées de F5 Networks, Inc. Toutes les autres marques ou noms de produits sont des marques commerciales ou des marques déposées de leurs propriétaires respectifs.

FirePass - L'accès distant sécurisé

FirePass - L'accès distant sécurisé



FirePass

L'accès distant sécurisé

Les entreprises se trouvent aujourd'hui confrontées à un problème de plus en plus complexe et frustrant : comment offrir un accès sécurisé, fiable et approprié aux applications, depuis n'importe quel dispositif Web et quelque soit l'utilisateur.

La solution idéale serait de permettre à tout utilisateur, quelque soit le client Web utilisé, d'obtenir les droits d'accès aux applications de l'entreprise - sans sacrifier la sécurité.

F5 est le seul fournisseur proposant une solution VPN SSL complète, fiable et performante, offrant un accès distant aux applications d'entreprise et de bureautique depuis n'importe quel poste client capable de se connecter au Web. Expert des technologies SSL et de la gestion du trafic applicatif, F5 fournit son savoir-faire aux entreprises désireuses de sécuriser et contrôler l'accès à leurs applications quelque soit le dispositif ou le lieu de connexion.

Points forts

- Facilité d'utilisation** – Le système dédié s'installe rapidement, offre une interface intuitive et familière (de type navigateur); utilise les technologies standards de chiffrement SSL et de navigation sur le Web pour gérer les problèmes d'accès ce quelque soit l'environnement de l'utilisateur.
- Fiabilité** – L'accès distant via le Web fonctionne et avec tous les fournisseurs d'accès Internet derrière d'autres firewalls, et opère entièrement sous HTTPS, le protocole Internet pour la sécurité des applications.
- Sécurité renforcée** – La sécurité au niveau de l'application est assurée; permet le chiffrement standard RC4 3DES pour des communications sécurisées.
- Coûts réduits** – Grâce à l'absence de logiciel client, le coût global de la solution est considérablement réduit. La maintenance des systèmes clients est éliminée; aucune modification aux ressources réseau, aux dispositifs d'accès clients ou à l'architecture réseau ne sont nécessaires.
- Règles d'administration** – Offre un contrôle granulaire utilisant les groupes, les droits d'accès et l'audit de comptes
- Une solution complète** – F5 propose une gamme de produits offrant une couverture intelligente de bout en bout pour les utilisateurs distants, le trafic IP et les applications basées sur IP - assurant haute disponibilité, capacités de montée en charge, sécurité et performances

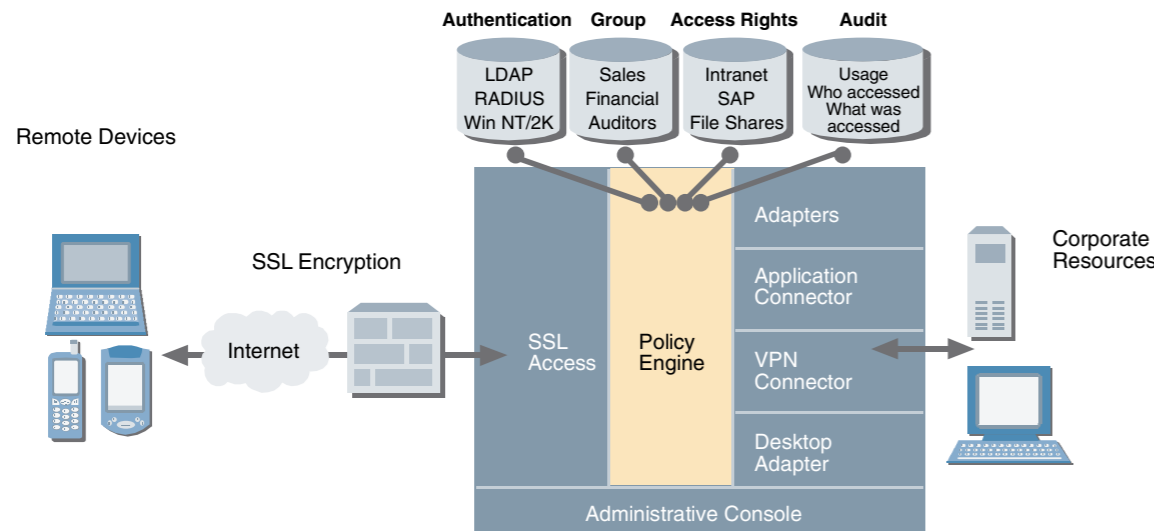
La problématique

Les entreprises exploitant des réseaux privés IPSec (ou VPN pour Virtual Private Networks) font face à des problèmes liés à l'adressage IP : la traduction des adresses réseau, un support limité des dispositifs distants, l'installation et la maintenance des applications et, plus particulièrement, la frustration des utilisateurs incapables d'accéder de façon fiable aux informations et applications dont ils ont besoin.

La solution

FirePass de F5 offre un accès distant fiable à quiconque peut se connecter à l'Internet - sans aucun logiciel ou configuration spécifique sur le client distant, et sans aucun ajout ou modification à l'application ou à la ressource accédée. Cette approche permet d'éliminer la charge que constitue le support du VPN IPSec et apporte l'accès le plus abouti et le plus complet aux e-mails, applications et pour la prise de contrôle à distance de PC de bureau à travers n'importe quel navigateur Web standard.

FirePass – L'accès distant sécurisé



MOTEUR DE RÉGLES DYNAMIQUES - LE CONTRÔLE ADMINISTRATIF TOTAL

Le moteur de règles de FirePass permet aux administrateurs de gérer facilement l'authentification des utilisateurs et les droits d'accès.

Accès dynamique basé sur des règles

Les administrateurs FirePass disposent d'un contrôle rapide et granulaire sur leurs ressources réseaux. Grâce à des règles, les administrateurs peuvent autoriser l'accès aux applications en fonction de l'utilisateur et du dispositif de connexion utilisé. Par exemple, les administrateurs peuvent configurer un profil d'utilisateurs pouvant accéder aux e-mails depuis un kiosque public, mais leur donner un accès complet aux ressources du réseau dès lors qu'ils se connectent sur un poste de travail de l'entreprise.

Authentification des utilisateurs

Par défaut, les utilisateurs s'authentifient vis à vis d'une base de données interne au FirePass, en utilisant leurs mots de passe. FirePass peut également être configuré pour exploiter les méthodes d'authentifications RADIUS et LDAP, l'authentification HTTP de base et par formulaire, et les serveurs de domaine Windows.

Services d'audit

FirePass fournit des rapports basés sur les journaux de sessions et d'activations. Les rapports de synthèse regroupent les volumétries d'utilisation par jour de la semaine, période de la journée, système d'exploitation accédé, fonction utilisée, site Web accédé, durée de la session, mode de fin de la session et autres informations au cours d'une durée de temps paramétrable par l'utilisateur.

Authentification à deux facteurs

De nombreuses entreprises exigent une identification à l'aide de "deux facteurs" - c'est à dire utilisant une autre méthode au delà de la connaissance de l'identifiant et du mot de passe. FirePass supporte complètement l'authentification RSA SecurID(r) basée sur les jetons. FirePass intègre également une implémentation de VASCO Digipass(r).

Gestion des droits d'accès

Les droits d'accès peuvent être attribués à des individus ou à des groupes d'utilisateurs (par exemple "Ventes", "Partenaires" ou "Informatique"). FirePass peut donc limiter les utilisateurs et les groupes à des ressources particulières. On peut ainsi accorder au groupe Partenaires un accès limité à un serveur d'extranet, tandis que les membres du groupe Ventes peuvent accéder aux e-mails, à l'intranet de l'entreprise et à l'application de CRM.

Stratégies dynamiques avec les certificats côté client

FirePass donne aux administrateurs la possibilité de restreindre ou d'autoriser l'accès en fonction du dispositif utilisé pour la connexion au système FirePass. FirePass peut également vérifier la présence d'un certificat numérique sur le client lors de l'authentification de l'utilisateur - ce certificat ne peut être présent que sur un seul ordinateur portable. Sur la foi de ce certificat, FirePass peut supporter l'accès à une plus large palette d'application.

Personnalisation de l'interface utilisateur

Les administrateurs peuvent modifier l'apparence de la mire d'accueil au FirePass et des écrans de détail, afin de les faire correspondre à la charte graphique de l'entreprise.

ADAPTATEURS FIREPASS - ACCÈS SÉCURISÉ DEPUIS LES SYSTÈMES PUBLICS

Les utilisateurs de kiosques ou d'ordinateurs domestiques (systèmes publics) sont des employés qui nécessitent l'accès aux ressources de l'entreprise depuis un dispositif qui n'est ni fourni, ni maintenu par l'entreprise. Pour ces utilisateurs, les adaptateurs FirePass offrent l'accès à une large gamme d'applications et de ressources du réseau. Chaque adaptateur représente une fonction distincte qui traduit l'application servie dans le langage du navigateur Web.

Adaptateurs disponibles pour FirePass:

Adaptateur Web

- Offre l'accès aux serveurs Web internes, notamment Microsoft Outlook Web Access, aussi facilement que depuis le LAN de l'entreprise.
- Tout en offrant l'accès aux ressources, FirePass assure une protection contre les attaques extérieures en mappant dynamiquement les URL internes à des URL externe ne révélant rien sur la structure interne.
- Une fois que la session de l'utilisateur est interrompue, FirePass peut dynamiquement supprimer l'historique de l'URL, les cookies utilisateurs et les fichiers cache/temporaires du navigateur afin de préserver la confidentialité et d'éviter de laisser des données sensibles sur le système public.
- Surveille les accès aux serveurs de l'intranet et détecte/empêche les attaques par scripts à travers le site.

FirePass – L'accès distant sécurisé



Adaptateur Terminal Server

- Assure l'accès via le Web aux serveurs Microsoft Windows Terminal Servers, aux applications Citrix MetaFrame, aux bureaux distants Windows XP et aux serveurs VNC.
- Supporte les options de groupes d'accès, l'authentification par signature unique, les fonctions d'authentification et de connexion automatiques pour les utilisateurs autorisés.
- Supporte le téléchargement et l'installation automatique des services Windows Terminal Services ou des composants client de plates-formes Citrix distantes, s'ils ne sont pas déjà installés sur le dispositif d'affichage - d'où une économie de temps.

Adaptateur pour PC de bureau

- Permet la prise de contrôle à distance sécurisée des postes de travail de l'entreprise.
- Offre la possibilité de partager le poste de travail avec d'autres utilisateurs pour la collaboration ou des démonstrations sur le Web; permet l'accès aux fichiers, aux e-mails et aux applications.

Adaptateur pour Systèmes Unix

- Supporte l'accès sécurisé aux postes de travail Unix/Linux.
- Utilise X Windows pour communiquer avec les applications Unix.

Adaptateur Host

- Permet l'accès via le Web aux applications héritées VT100, VT320, Telnet, X-Term, et IBM(r) 3270/5250.
- Ne nécessite aucune modification sur les applications ou sur les serveurs d'applications.

Adaptateur File Server

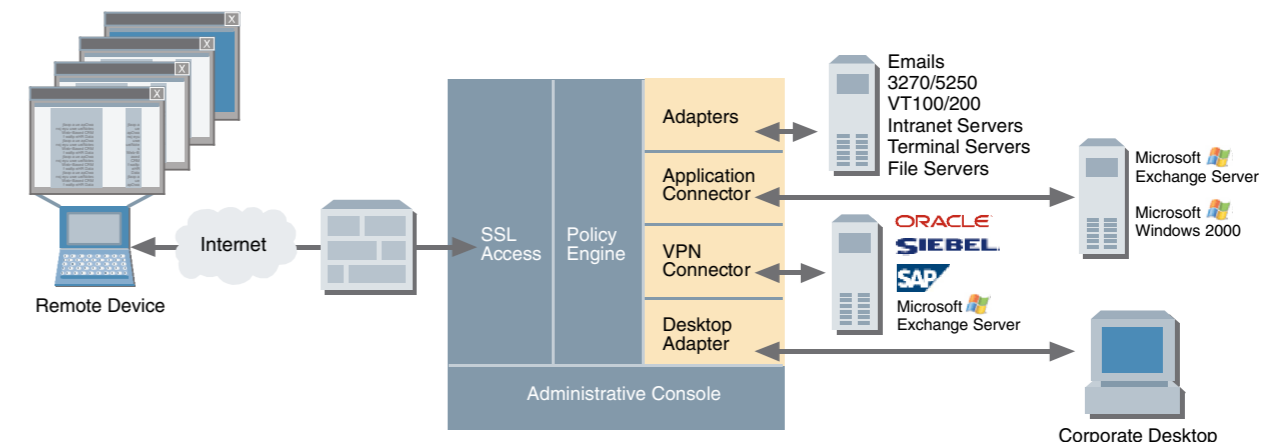
- Permet aux utilisateurs de naviguer, télécharger, copier, déplacer ou effacer des fichiers sur les répertoires partagés.
- Supporte les partages SMB, les groupes de travail Windows; les domaines Windows NT 4.0 et Windows 2000; Novell(r) 5.1/6.0 avec le pack Native File System et les serveurs NFS.

Adaptateur e-mail

- Assure l'accès aux serveurs d'e-mails POP/IMAP/SMTP et aux carnets d'adresses LDAP à l'aide d'un simple navigateur Web.
- Permet aux utilisateurs d'envoyer et recevoir des messages, de télécharger des attachements et d'attacher des fichiers du réseau en pièces jointes aux e-mails.

Adaptateur Mobile

- Support des PDA tels que les systèmes sous Palm OS, les téléphones cellulaires tels que le WAP et les téléphones iMode.
- Accès aux fichiers, e-mails et données PIM, affichage des documents Word et des fichiers PDF sur les organisateurs ou les téléphones Internet.



ACCÈS SÉCURISÉ AUX PARTENAIRES

Un partenaire commercial est une personne non employée par l'entreprise et utilisant un équipement fourni et maintenu par une autre société dont les normes sont inconnues. FirePass permet aux administrateurs d'affecter à ces utilisateurs des droits d'accès aux applications et sites de l'extranet via l'adaptateur Web. L'adaptateur protège les ressources du réseau en ne permettant l'accès qu'aux sites Web autorisés spécifiquement par l'administrateur système.

Contrôle d'accès sélectif

Afin de permettre aux partenaires un accès sélectif aux applications client-serveur, FirePass offre le connecteur d'applications. Il permet aux administrateurs d'attribuer des droits d'accès à des applications du réseau sans pour autant offrir aux partenaires un accès à la totalité du réseau.

Le connecteur d'applications FirePass :

- Supporte l'accès des clients distants aux serveurs d'applications.
- Permet à une application native côté client de communiquer en retour avec le serveur d'applications de l'entreprise via un canal sécurisé entre le navigateur et le système FirePass.
- Permet aux utilisateurs de "mapper" les unités du LAN sur le système distant.
- Ne demande à l'utilisateur aucune installation préalable ou configuration de logiciel.
- Sur le plan réseau, ne nécessite aucun logiciel supplémentaire sur les serveurs d'applications accédés.
- Utilise le protocole standard HTTPS, avec SSL pour le transport et peut donc fonctionner à travers tous les proxy HTTP - les points d'accès publics, les réseaux LAN privés et sur les réseaux et les FAI ne supportant pas les VPN IPSec traditionnels.
- Les connecteurs standards incluent les clusters Outlook ou Exchange, FTP et Citrix Nfuse. Les administrateurs peuvent créer des connecteurs pour les applications utilisant les ports TCP statiques.