

Security

FirePass®

情報の活用と保護を同時に実現し、ビジネスの効率アップ！

社内アプリケーションへアクセスするデバイスやロケーションの多様化に伴い、柔軟で生産性の高い作業環境がビジネスの収益性向上には欠かせません。しかし、不正アクセスや攻撃からアプリケーション、データ、ネットワーク、およびクライアントデバイスをセキュリティで保護すると管理は複雑になり、新しい脅威が登場するたびにコストも増加していきます。

FirePass は、あらゆるデバイスやネットワークからエンタープライズ・アプリケーションおよびデータへのセキュアなリモートアクセスを提供。パフォーマンス、拡張性、可用性、ポリシー管理、およびエンドポイント・セキュリティに優れた FirePass が、セキュリティ強化、アクセス制御、社員の生産性と機動性の向上を実現します。

目次

- 1 主な特長
- 2 ネットワークアクセス
- 4 アプリケーション・アクセス – 特定のアプリケーションに対するセキュアなアクセス
- 6 ポータルアクセス – Web アプリケーション、ファイル、Eメールへのプロキシベース・アクセス
- 7 ポータルアクセス – 包括的なセキュリティ
- 8 動的ポリシーエンジン – 包括的な管理制御
- 9 カスタマイズ
- 10 セキュアなアプリケーション・アクセスに対する iControl SSL VPN クライアント API
- 10 製品情報
- 11 ハードウェア仕様

主な特長

社員の生産性の向上

あらゆるロケーションの各種デバイスからのセキュアなリモートアクセスを実現します。

コスト削減

使いやすく導入が簡単な FirePass は、セキュアなアプリケーション・アクセスを実現して導入コストおよびサポートコストを低減します。

セキュリティの強化

グループベースでインターネットリソースに詳細なアクセス制御を提供します。

エンドポイント・セキュリティ

エンドポイント・セキュリティでユーザを簡単かつ速やかに確認して、企業ポリシーの準拠を検証します。

FirePass の機能

- クラス最高のポリシー管理 – 独自のビジュアルポリシーエディタには簡単に操作できるインターフェイスを備え、詳細なアクセスポリシーを管理しながら管理コストを削減。ログオン前ポリシーのインポート/エクスポートにより、管理者が既存のポリシーを容易に管理・実施することができます。
- グループポリシー・エンフォースメント – ネットワークドメイン外のクライアント・システムでグループポリシーを適用・実行するための専用メカニズムを提供。テンプレートという形で提供されるポリシーが、クライアントにおけるユーザの権限とアクセスを制限しつつ、PCI、HIPAA、GLBA への準拠を徹底させます。
- 統合型のエンドポイント・セキュリティ – セキュアな仮想ワークスペース、ログイン前のエンドポイント整合性チェック、およびエンドポイントの信頼性管理を提供することで、管理を簡素化します。
- 広範なアプリケーション・サポート – E メール、Web ポータル、ネットワークファイル・サービス、ターミナルサービス、CRM および他の主要なエンタープライズ・アプリケーションにあらゆるデバイスを使ってアクセスできます。
- 広範なクライアントサポート – FirePass は複数のプラットフォームをサポートし、Windows (2000、XP、Vista)、Linux、Mac、Apple iPhone、Windows Mobile、その他のスマートフォンからのセキュアなネットワークアクセスを実現します。
- エンタープライズ級の拡張性とパフォーマンス – 管理のしやすい1台のデバイスで最大 2,000 接続の同時セッションをサポート。F5 の BIG-IP Local Traffic Manager およびクラスターリング機能との統合により、世界的な展開に対応するための拡張が容易に行えます。あらゆる IP アプリケーション・トラフィックの圧縮や Web アプリケーションのサーバ側でのキャッシングといった機能を利用して、エンドユーザ・エクスペリエンスを最適化します。
- 広範囲な相互運用性 – 既存のネットワーク・インフラストラクチャに対応し、RADIUS や LDAP、PKI、RSA などを介して管理システムを特定。また、Java アプレット、JavaScript の変更などをサポートしている統合 Web ポータルの使用を実現 (VPNC 認定)。
- 業界をリードするグローバルなハイアベイラビリティ – F5 独自の BIG-IP Global Traffic Manager との統合によって、サイトに障害が発生しても WAN 全体でハイアベイラビリティを維持。フェイルオーバーサポートによってサイト内にハイアベイラビリティを提供。

ネットワークアクセス

Windows (2000/XP/Vista)、Mac、Linux システムをサポートする FirePass ネットワークアクセス

- Windows インストーラー・サービスにより、FirePass クライアント・コンポーネントのアップデートの際に特別な管理権限が不要になり、管理コストが削減されます。
- ネットワーク全体で、IP ベース (TCP、UDP) のアプリケーションに安全なリモートアクセスを提供します。
- ラップトップ・プラットフォームのスプリットトンネリング、圧縮、アクティビティベースのタイムアウト、自動アプリケーション起動などの標準機能を提供します。
- IPsec VPN とは異なり、リモートアクセスにプリインストールされたクライアント・ソフトウェアやリモートデバイスの設定は必要ありません。クライアント側、サーバ側のアプリケーションともに変更する必要はありません。
- 管理者は、特定のネットワークやポートへのアクセスを制限するルールを作成することで、アクセスできるリソースを制限または保護することができます。
- 標準の HTTPS プロトコルと、転送用に SSL を使用することで、パブリック・アクセスポイント、プライベート LAN、IPsec VPN をサポートしないネットワークや ISP など、すべて HTTP プロキシで動作させることができます。
- GZIP 圧縮を使用して暗号化される前にトラフィックを圧縮し、インターネットで送信するトラフィックの量を軽減します (パフォーマンスが改善します)。

クライアント・セキュリティ

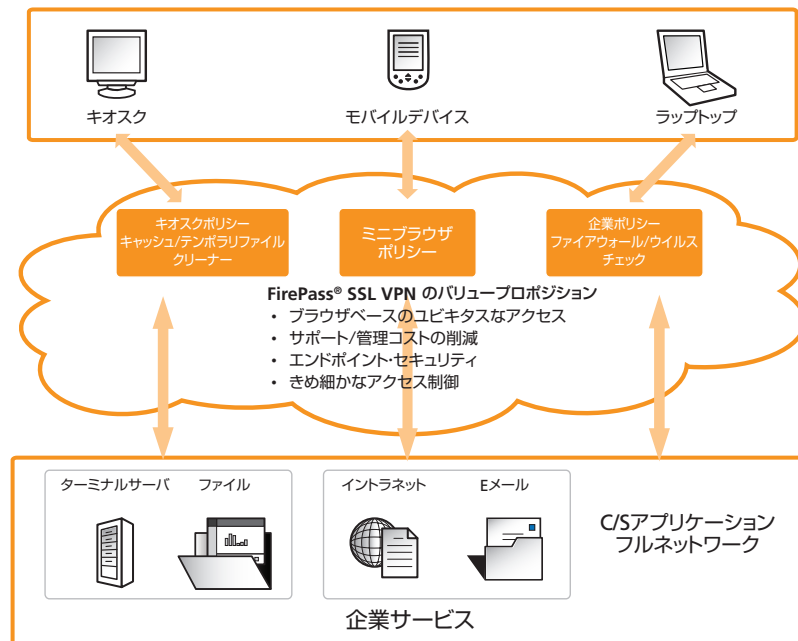
- セーフ・スプリット・トンネリング – スプリット・トンネリングを使ってネットワークにアクセスする場合のバックドア攻撃を防ぐために、FirePass はフルネットワーク・アクセス機能使用時に Windows 2000/XP/Vista、Mac、Linux ユーザを保護する動的なファイアウォールを提供します。この機能を使用すると、クライアントを介して社内ネットワークに接続するハッカーのルーティングを防ぐことができます。また、意図せずパブリック・ネットワークにトラフィック送信することもなくなります。
- クライアントの総合チェック – ネットワークアクセスを完全に許可する前に、クライアントのコンピュータに必要なプロセス（ウイルススキャン、パーソナル・ファイアウォール、OS パッチレベル、レジストリ設定など）が存在しているかどうか、または不要なプロセス（キーストロークを悪用するプログラムなど）が存在しているかどうかを検出することで、セキュリティを強化しています。

ネットワークアクセス機能

- スタンドアロン Windows クライアント – ユーザは認証内容を入力したあと、FirePass によってネットワーク接続が確立します。ソフトウェアは、Microsoft の MSI インストーラ・テクノロジーによってクライアントに自動配信されます。
- Windows ログオン/GINA 統合 – GINA(“ctrl + alt + del” プロンプト) ログオンプロセスの統合により、企業ネットワークへの暗黙的かつ透過的なユーザログオンを実現します。
- スタンドアロン VPN クライアント CLI – サードパーティ・アプリケーション（リモートダイヤル・ソフトウェアなど）との統合により、新しいコマンドライン・インターフェイスでのシングル・サインオンを実現。
- Windows VPN ダイアラー – ダイアルアップ・インターフェイスを使い慣れたユーザ向けに、簡単なエンドユーザ操作性を提供。
- 自動ドライブマッピングの提供 – ネットワークドライブを、ユーザの Windows コンピュータに自動的にマッピングできます。
- 静的 IP サポートの提供 – ユーザがネットワークアクセスの VPN 接続を確立した場合、ユーザに基づいて静的 IP を割り当てます（管理者の負荷を軽減できます）。
- 透明なネットワークアクセス – ネットワークアクセス・ブラウザウィンドウのポップアップ表示を禁止することで、ユーザが誤って接続を切断しないようにします。

モバイルデバイスのサポート

- Windows Mobile やスマートフォンからのセキュアなアプリケーションアクセス
- クライアント / サーバと Web ベースのアプリケーションの両方へのアクセス



アプリケーション・アクセス – 特定のアプリケーションに対する安全なアクセス

管理者は、特定の外部アプリケーションやサイトへアクセスするユーザを制限できます（会社で管理されていない機器を使用しているビジネスパートナーなど）。FirePass は、システム管理者が個別に認証したアプリケーションのみにアクセスを許可することで、ネットワークリソースを保護します。

特定のクライアント / サーバ・アプリケーションへのアクセス

- ブラウザと FirePass コントローラ間の安全な接続を使用して、ネイティブ・クライアント側のアプリケーションと会社の特定のアプリケーション・サーバを通信させることができます。
- ユーザ側はソフトウェアのプリインストールや設定を行う必要はありません。
- ネットワーク側で、アクセスするアプリケーション・サーバで新たに有効にするソフトウェアはありません。
- ネットワークアクセスと同様、HTTP と SSL/TLS の標準プロトコル経由でアプリケーションにアクセス。この機能は、従来の IPsec VPN をサポートしていないあらゆる HTTP プロキシ、アクセスポイント、プライベート LAN、ネットワーク、ISP で有効に動作します。
- Outlook から Exchange までアプリケーションをサポートします (Passive FTP、Citrix Nfuse、およびネットワークドライブ・マッピング)。
- 管理者は、CRM や他の静的 TCP ポートを使用するアプリケーションをカスタマイズすることもできます。
- App トンネル、Citrix、WTS アプリケーションへの自動ログインをサポートし、エンドユーザの負担を軽減します。
- クライアント側のアプリケーションを自動起動させることで、エンドユーザの負担やサポートコストを軽減します。

- 非 Windows システムおよびロックダウンした Windows システム用に Java ベースのアプリケーショントンネルを有効にし、ActiveX コントロールの実行を防止。
- ネットワークアクセスを利用するクライアントに対して完全な DHCP サポートを提供することで、IP アドレスの割り当てとアドレスのダイナミック DNS 登録を自動化。DHCP サポートによってマルチユニットの導入が簡素化されます。また、リモートアクセス IP アドレスの範囲が社内 LAN と重複しても問題ありません。
- ポータルアクセス経由で MS Communicator をサポートすることで、VoIP 通信が拡充されます。
- WAN 上でクライアント / サーバアプリケーションのトラフィックを独自に圧縮し、より最適なパフォーマンスを提供します。

ターミナルサーバ・アクセス

- Microsoft ターミナルサーバ、Citrix MetaFrame アプリケーション、Windows XP のリモートデスクトップ、および VNC サーバに安全な Web ベースのアクセスを提供します。
- グループアクセス・オプション、ユーザ認証と自動ログイン機能、または権限のあるユーザをサポートします。
- ターミナルサービスまたは Citrix リモート・プラットフォームのクライアント・コンポーネントを適切にダウンロードしてインストールできます。リモートデバイスにインストールされていない場合など、時間を節約できます。
- RDP を使用した Windows XP デスクトップへのリモート・トラブルシューティングのリモートアクセスや、VNC 機能を使用した非 Windows XP デスクトップのリモートアクセスをサポートします。
- Citrix と Microsoft 用に Java ベースのターミナルサービスをサポート。

ダイナミック App トンネル

- 多様なクライアント / サーバ・アプリケーションと Web ベースのアプリケーションへのアクセスを幅広くサポート。
- Windows クライアントデバイスからアプリケーションへのアクセスのためのリバースプロキシよりも適切な方法。
- Web アプリケーション・コンテンツとの互換性テストは不要。
- 利用時には「パワーユーザ」権限のみ必要で、実行のための特殊な権限は不要。
- Web アプリケーション・トンネリングの自動起動をサポートすることで、エンドユーザの操作性を改善しています。

ホストアクセス

- 旧来の VT100、VT320、Telnet、X-Term、IBM 3270/5250 アプリケーションに対して安全な Web ベースのアクセスを提供します。
- アプリケーションやアプリケーション・サーバに修正を加える必要はありません。
- サードパーティ製のホストアクセス・ソフトウェアは必要なく、TCO の削減につながります。

ポータルアクセス – Web アプリケーション、ファイル、E メールへのプロキシベース・アクセス

FirePass のポータルアクセス機能は、ブラウザを搭載したあらゆるクライアント OS (Windows、Linux、Macintosh、スマートフォン、PDA など) で有効に動作します。

Web アプリケーション

- Microsoft Outlook Web Access、Lotus iNotes、Microsoft SharePoint Portal Server など、社内 LAN と同じように簡単に内部 Web サーバへアクセスできます。
- グループベースでインターネットリソースに詳細なアクセス制御を提供します (例: 社員はすべてのイントラネットサイトにアクセスさせる一方、パートナーのアクセスは特定の Web ホストに制限)。
- リソースにアクセスを提供しながら、FirePass は内部 URL から外部 URL へ動的にマッピングし、内部ネットワーク構造を外部に知られることを防ぎます。
- FirePass コントローラでユーザの Cookie を管理することで、重要な情報の流出を防ぎます。
- ユーザの認証内容を Web ホストに渡すことで自動ログインでき、他のユーザも特定のアプリケーションにアクセスできるようになります。また、FirePass が既存の ID 管理サーバ (例: Netegrity) を統合するため、アプリケーションヘシングルサインオンを実行できます。
- Web ホストからのログイン要求をプロキシすることで、ユーザが自身のパスワードをクライアントブラウザにキャッシュさせることを防ぎます。
- きめ細かい ACL (Access Control List) によって、アプリケーションの特定部分へのアクセスを制限し、セキュリティ向上とビジネス上のリスク軽減を実現。
- Web アプリケーションのスプリット・トンネリングをサポートすることで、公開している Web サイトへのアクセス時のユーザパフォーマンスを向上させます。
- ラピッド・リバースプロキシ・バックエンド証明書認証機能が、サーバの証明書をすばやく認証。
- サーバ側の動的な DNS キャッシングにより、Web アプリケーション (リバースプロキシ) のパフォーマンスの向上とページダウンロード時間の短縮が実現。
- 独自のリバースプロキシをサポートし、さまざまな Web ページの JavaScript コンテンツを書き換えることで時間を節約します。
- FirePass のポータルアクセス機能を使うことで、クライアント主導の接続を制限する Java パッチ ACL をサポート。
- Web アプリケーションへのアクセス用に NTLMv2 をサポート。
- DNS プロキシサービスを提供。これによって、特別なランタイム権限 (ホストファイルの変更など) がなくてもクライアント側でネームリゾリューションを実行することができます。またポートのリダイレクションも可能になり、Outlook や Windows ドライブマッピングなどのアプリケーションがフルにサポートされます。

ファイルサーバ・アクセス

- ユーザに、共有ディレクトリのファイルの参照、アップロード、ダウンロード、コピー、移動、削除を許可します。
- SMB を使ったファイル共有サービス、Windows Workgroup (NT 4.0 および Windows 2000 ドメイン)、Novell 5.1/6.0 Native File System Pack をサポートします。

E メールアクセス

- 標準のブラウザやモバイルデバイスのブラウザから、安全な Web ベースのアクセスを POP/IMAP/SMTP の E メールサーバに提供します。
- E メールでメッセージの送受信、添付ファイルのダウンロード、ネットワークファイルの添付を実行できます。

モバイルデバイス・サポート

- Apple iPhone、Windows Mobile、PDA、スマートフォン、携帯電話、WAP、iMode 携帯電話から Web ベースのアプリケーション (E メールなど) へのアクセスを実現。
- POP/IMAP/SMTP の E メールサーバからの Eメールのフォーマットをダイナミックに変更し、携帯電話や PDA のような小さい画面に合わせます。
- Eメールの添付ファイルとしてネットワークファイルを送信し、テキストまたは Word 文書を表示できます。
- ActiveSync のサポート – ActiveSync アプリケーションのサポートにより、PDA デバイスに VPN クライアント・コンポーネントを事前にインストールすることなく、PDA が Exchange サーバ上の Eメールやカレンダーに同期できるようになります。

ポータルアクセス – 包括的なセキュリティ

FirePass は、公開のシステムからの情報アクセスに安全性を持たせるため、複数のレイヤ制御を行います。

クライアント・セキュリティ

- プロテクトド・ワークスペース – Windows 2000/XP/Vista ユーザは、リモートアクセス・セッション時に、自動的にプロテクトド・ワークスペースに切替えられます。プロテクトド・ワークスペース・モードでは、ユーザはプロテクトド・ワークスペース以外でファイルに書き込むことができなくなります。さらに、テンポラリフォルダやそのコンテンツは、セッション終了時にすべて削除されます。
- キャッシュ・クリーンアップ – キャッシュ・クリーンアップ制御は、クッキー、ブラウザの履歴、オートコンプリート情報、ブラウザのキャッシュ、テンポラリファイル、およびリモート・アクセス・セッション時にインストールされたすべての ActiveX コントロールを削除し、ごみ箱を空にします。
- セキュアな仮想キーボード – パスワードによるセキュリティを追加する場合、FirePass では仮想セキュリティ・キーボード (特許申請中) を使用できます。セキュアな仮想キーボードは、キーボード入力の代わりにマウスを使用してパスワードを安全に入力する機能です。
- ダウンロードブロック – システムに「クリーンアップ」コントロールをインストールできない場合、FirePass は予期せぬ問題に備えるためダウンロードファイルをブロックするように設定ができます (アプリケーションへのアクセスは可能です)。

コンテンツ検査と Web アプリケーション・セキュリティ

社内ネットワークの Web アプリケーションにアクセスするユーザに対して、アプリケーション・セキュリティを強化しました。Web アプリケーション・アクセスをスキャンすることで、アプリケーション・レイヤ攻撃 (例: クロスサイト・スクリプティング、無効な文字、SQL インジェクション、バッファ・オーバーフロー) を防ぎます。また攻撃が検出されると、ユーザアクセスをブロックします。

ウイルス保護機能の統合

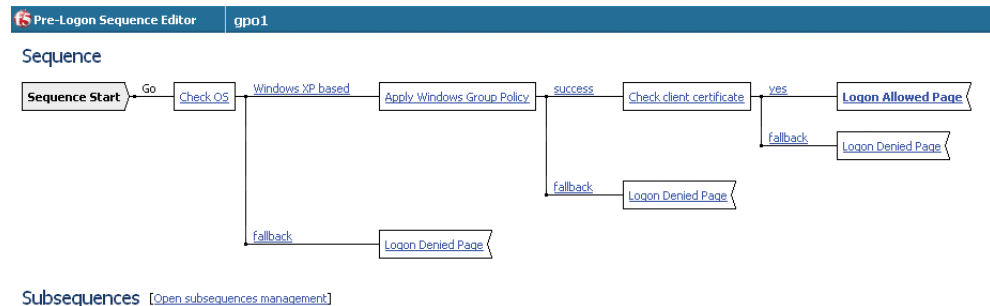
FirePass は、ICAP API 経由で統合スキャナまたは外部スキャナを使用して、Web やアップロードするファイルをスキャンできます。感染したファイルはゲートウェイでブロックされます。さらに、セキュリティを高めるため、ネットワークの Eメールサーバまたはファイルサーバでそれらのファイルは拒否されます。

動的ポリシーエンジン – 包括的な管理制御

FirePass のポリシーエンジンを使用することで、管理者はユーザ認証と権限許可を簡単に管理できます。

ポリシーベースの動的アクセス

管理者はネットワークリソースを迅速かつきめ細かに制御することができます。ポリシーのサポートによって、ユーザおよび使用中のデバイスに基づきアプリケーションへのアクセスを許可することができます。管理者は、プレログオンポリシーをインポート/エクスポートすることで、既存のポリシーを容易に実行することができます。



ビジュアルポリシーエディタのユニークな機能の 1 つに、グラフィカルなフローチャート形式を使用したアクセスポリシー作成機能があります（クリックするだけで簡単にプロファイル作成をしたり、グループやユーザ、デバイス、またはそれらを組み合わせたものを管理できます）。このエディタを使用することで、エンドポイント・ポリシーの定義や管理を簡易化したり、管理者の負担を軽減するため、会社のリソースを迅速に保護できます。

ユーザ認証

デフォルトでは、パスワードを使って FirePass の内部データベースと照合し、ユーザの認証が行われるようになっています。しかし、簡単な設定によって、RADIUS、Active Directory、RSA 2-Factor、LDAP の各種認証方式、フォームベースのベーシックな HTTP 認証、アイデンティティ管理サーバ (Netegrity など)、および Windows ドメインサーバと連携させることもできます。Active Directory によって、ユーザは現在のパスワードや期限切れのパスワードを変更することができ、またパスワードの期限が切れた時点で警告を受け取ることもできます。Active Directory のネスト構造がサポートされていることで、より複雑な階層型のディレクトリ構造を利用することができます。

2 ファクタ認証

多くの企業が、ユーザ ID およびパスワード以外のものを使用した「2 ファクタ」認証を必要としています。FirePass は、RSA の SecurID® トークンベース認証および RSA ネイティブ ACE 認証を完全にサポートしています。

クライアント側の証明書 / PKI のサポート

管理者は、FirePass コントローラへのアクセスに使用したデバイスに基づいて、アクセスを制限または許可することができます。FirePass は、ユーザのログイン中にクライアント側のデジタル証明書を確認できるためです。デジタル証明書があると、FirePass はアプリケーションのアクセス範囲をより広くサポートできます。また、FirePass は、クライアント側の証明書を 2 ファクタ認証の 1 つとしても使用できるため、有効なクライアント側の証明書がない場合、すべてのネットワークアクセスを禁止することもできます。

グループ管理

ユーザごと、またはグループ（例：セールス、パートナー、IT）ごとにアクセス権限を設定できます。これにより、特定のリソースに対してユーザとグループのアクセスを制限します。

ダイナミック・グループマッピング

Active Directory、RADIUS、LDAP、クライアント証明書、URI、仮想ホスト名、ログオン前のセッション変数など、各種の動的グループマッピング技法を使用し、FirePass はユーザを各グループに動的にマッピングします。

Single Sign On (SSO) のサポート

SSO 設定では、認証セッション変数を使って、証明書から SSO 情報としてユーザ名とパスワードを取得し、認証を行います。高度なセッション変数により、システム管理者は FirePass を拡張・カスタマイズすることができ、新しいセッション変数を操作・作成してカスタムの導入を行うことができます。また、RADIUS 属性に加えて、LDAP、AD、証明書のフィールド値を収集・取得することもできます。

セッションのタイムアウトと制限

管理者は非アクティブ・タイムアウトとセッション・タイムアウトを設定することで、キオスクでログオフし忘れたセッションに対するハッカーのハイジャックを防ぐことができます。

役割ベースの管理

役割ベースで管理することで、企業の構成に柔軟に対応できます。管理機能（新規ユーザの登録、セッションの終了、パスワードの再設定）を他の管理者に提供する場合、すべての機能を公開する必要がありません（サーバのシャットダウン、証明書の削除など）。

ロギング & レポート

FirePass には、ユーザ、管理者、セッション、アプリケーション、システムイベントを記録するためのロギング機能が内蔵されています。また、FirePass は標準的なフォーマットでログを提供することから、外部の syslog サーバとの統合を実現します。管理コンソールでは多様な監査レポートが提供され、複数のセキュリティ監査に対応できるようになっています。サマリーレポートは、ユーザが指定する時間間隔の利用状況を、曜日、時間、アクセスを行う OS、使用する機能、アクセス先の Web サイト、セッション時間、セッション終了の種類、およびその他の情報ごとにまとめたものです。1 つの URL を使って、HTML もしくはスプレッドシート・フォーマットのサマリー / グループレポートを読み出すことができます。

カスタマイズ

エンドユーザの GUI の日本語化

FirePass では、機能名 (Web アプリケーションなど) を始めとするエンドユーザ Web ページのすべてのフィールドをローカライズすることができます。これによって企業は、ユーザのお気に入りだけでなくエンドユーザの GUI もあわせてローカライズすることができ、ビジネス価値の向上と TCO の削減につながります。

ログインとウェブトップ全体のカスタマイズ

管理者は FirePass を使用して、ログインとウェブトップの Web ページ全体を、既存の企業の Web サイトポータルに合わせてカスタマイズできます。エンドユーザのレベルに応じて、WebDAV 機能を使用してカスタマイズしたページをアップロードできます。

セキュアなアプリケーション・アクセスに対する iControl SSL VPN クライアント API

FirePass はオープンクライアントの API と SDK を搭載した唯一の SSL VPN 製品であり、セキュアなシステム間通信やアプリケーション間通信を提供することで、Win32 クライアント OS (2000、XP、Vista) からのセキュアな自動アクセスを可能にします。今では、アプリケーションによってネットワーク接続が透過的に自動開始 / 終了することから、ユーザが VPN にログインする必要がありません。これによって、エンドユーザの接続が迅速かつ簡単に行えるばかりでなく、クライアント・アプリケーションの導入にかかるコストも削減されます。

製品情報

FirePass アプライアンスシリーズは 3 モデル展開となっており、小～大企業の同時ユーザアクセスのニーズに対応します。

FirePass 1200 シリーズ

FirePass 1200 アプライアンスは小中規模企業およびブランチオフィス向けに設計されており、10 ~ 100 人の同時ユーザをサポートします。

FirePass 4100 シリーズ

FirePass 4100 コントローラは中規模企業向けに設計されており、価格性能比の観点から見ると、最大同時ユーザ数 500 人程度の環境に適しています。

FirePass 4300 シリーズ

FirePass 4300 アプライアンスは中大規模企業およびサービスプロバイダ向けに設計されており、最大 2,000 人の同時ユーザをサポートします。

クラスタリング

FirePass 4100 と 4300 にはいずれもクラスタリング機能が内蔵されています。BIG-IP Global Traffic Manager と BIG-IP Local Traffic Manager を組み合わせることで、業界最高級の拡張性、パフォーマンス、安定性を提供します。

フェイルオーバー

FirePass アプライアンスでは 2 つのサーバ (アクティブサーバとスタンバイサーバ) 間のフェイルオーバーを設定することもでき、万が一プライマリユニットが停止した場合にもユーザがほかの FirePass に再ログインしなくてもすむようになっています。

SSL アクセラレータ・ハードウェア

FirePass 4100 は、SSL 鍵交換ならびに SSL トラフィックの暗号化 / 復号化をオフロードする独自のハードウェア SSL アクセラレーションを標準で提供します。これによって、大規模なエンタープライズ環境におけるパフォーマンスの飛躍的な向上が可能になり、プロセッサに負荷をかける暗号化 (3DES や AES など) にも対応することができます。

FIPS SSL アクセラレータ・ハードウェア・オプション *

FirePass は FIPS に準拠 * しており、政府、金融機関、医療機関といった、セキュリティが重視される組織の厳しいセキュリティニーズに対応します。FirePass 4100 と 4300 では、FIPS 140 Level-2 対応の SSL 鍵改ざん防止ストレージ、ならびにハードウェアでの SSL トラフィックの暗号化 / 復号化のための FIPS 認定暗号化がサポートされています。FIPS SSL アクセラレータは、ベースの 4100 と 4300 プラットフォームに対する工場出荷時インストールオプションとして提供されます。

* FIPS 140-2 は、プライベート・データ・トラフィックでの利用に関する CESG (英国の品質保証に関する国家技術委員会) のセキュリティ基準を満たしています。



FirePass 1200 シリーズ



FirePass 4100 & 4300 シリーズ

ハードウェア仕様	FirePass 1200	FirePass 4100	FirePass 4300
電源	シングルフルレンジ 250W	400W 90/240 +/- 10% VAC オートスイッチング 冗長電源オプション	デュアル 460W 90/240 +/- 10% VAC オートスイッチング
重量	10 lbs	40 lbs	43 lbs
外形寸法 (インチ)	H1.7、W16.7、D11 1U 業界標準ラックマウント・シャーシ	H3.5、W17.5、D23.5 2U 業界標準ラックマウント・シャーシ	H3.5、W17.5、D23.5 2U 業界標準ラックマウント・シャーシ
適合規格	UL 60950 (UL 1950-3)、CSA-C22.2 No 60950-00 (Bi-national standard with UL 60950) CB test certification to IEC 950、 EN 60950	UL 60950 (UL 1950-3)、CSA-C22.2 No 60950-00 (Bi-national standard with UL 60950) CB test certification to IEC 950、 EN 60950	UL 60950 (UL 1950-3)、CSA-C22.2 No 60950-00 (Bi-national standard with UL 60950) CB test certification to IEC 950、 EN 60950
動作時温度	5 ~ 40°C	5 ~ 40°C	5 ~ 40°C
相対湿度	20 ~ 90% (40°Cにて)	20 ~ 90% (40°Cにて)	20 ~ 90% (40°Cにて)



F5 ネットワークスジャパン株式会社

東京本社

〒107-0052 東京都港区赤坂 4-15-1 赤坂ガーデンシティ 19階
TEL 03-5114-3210 FAX 03-5114-3201

www.f5networks.co.jp/fc/

西日本支社

〒530-0001 大阪市北区梅田 2-2-2 ヒルトンプラザウエスト オフィスタワー 19階
TEL 06-6225-1250 FAX 06-6225-1111