HP IceWall SSO

HP IceWall技術レポート：SSL VPNアプライアンスとの連携 F5ネットワークス社 FirePass

はじめに

社外からイントラネットのサーバーにリモートアクセスする際に、SSL VPNアプライアンスが使われるケースが多くあります。
本レポートでは、SSL VPNアプライアンスにログインしたユーザーがHP IceWall SSOにID/パスワードを再入力せずにシームレスにログインする方法についてご紹介します。
本レポートでは、F5ネットワークス社のFirePass 4100とHP IceWall SSOの連携方法をご紹介します。

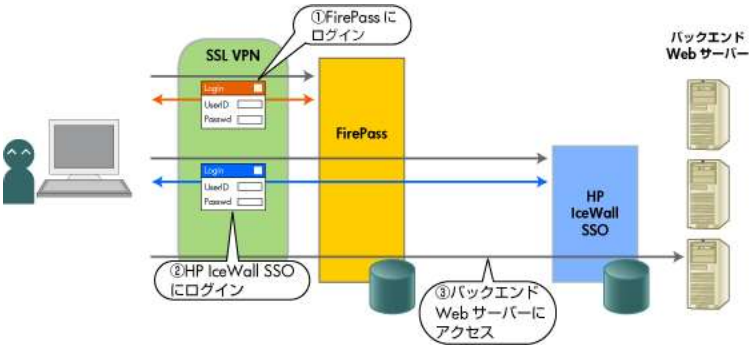
F5ネットワークス社 FirePass4100

F5ネットワークス社FirePass4100(以下 FirePass)は、従業員やパートナーのリモートアクセスを実現するためのSSL VPN アプライアンスです。
VPNのプロトコルとして、標準的なWebブラウザに搭載されているSSLを使用します。このため、特別なクライアントソフトの導入や内部サーバーの設定変更が不要です。
HP IceWall SSOとの連携には、FirePassの「HTTPフォームベース認証機能」を使用します。この機能は、FirePassがユーザーから受け取ったユーザーID/パスワードなどの認証情報をHTTPで外部のサーバーに送り、その結果によりユーザーのログインを許可する機能です。

FirePass 4100とHP IceWall SSOの連携のメリット

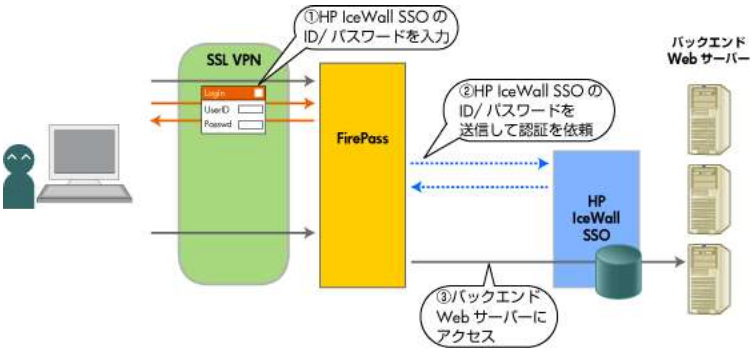
FirePassとHP IceWall SSOの認証を連携させない場合

ユーザーは、FirePassに登録されたユーザーID/パスワードを入力してFirePassにログインします。
その後、HP IceWall SSOのバックエンドWebサーバーにアクセスする際に、HP IceWall SSOの認証データベースに登録されたユーザーID/パスワードを入力してHP IceWall SSOにログインします。



FirePass4100とHP IceWall SSOの認証を連携させた場合

①ユーザーは、HP IceWall SSOに登録されたユーザーID/パスワードを入力してFirePassにログイン要求をします。
②FirePassはユーザーID/パスワードをHP IceWall SSOに送信し、認証を依頼します。ユーザーID/パスワードが正しければ、ユーザーはFirePassにログインできます。
③ログイン後はHP IceWall SSOを含めたFirePass配下のサービスをそのまま利用できます。



FirePass4100とHP IceWall SSOの連携方法

■ ユーザレポジトリ
ユーザーレポジトリはHP IceWall SSOの認証データベースを使用します。

- FirePass
  - FirePassの認証方式をHTTPフォームベース認証に設定し、HP IceWall SSOのログインURLを定義します。
  - 内部データベースにはユーザー登録は必要ありません。
- HP IceWall SSO
  - HP IceWall SSOの認証データベースとしてOracleを使用します。
  - 認証データベースには、HP IceWall SSOにログインするためのユーザー/パスワードを登録します。

■ 接続形態
FirePassからHP IceWall SSOにパスワードの問い合わせをするには、FirePassの認証方式をHTTPフォームベースに定義します。HTTPフォームベースの認証方式では、FirePassはユーザーから入力されたIDとパスワードをもとにHTTPリクエストを生成し、問い合わせ先のWebサーバー(＝今回の場合はIceWallサーバー)に中継します。
さらにFirePassの「Webアプリケーションお気に入り設定」に、HP IceWall SSOのトップ画面(ポータル画面等)を登録することで、FirePassを経由してHP IceWall SSOに、そのまま認証なしでアクセスができるようになります。

※「Webアプリケーションお気に入り設定」は、FirePass経由で使用できるアプリケーションの一つとして、HP IceWall SSOなどのWebサーバー(URL)を登録する設定です。詳細はFirePassのマニュアル等を参照してください。

■ HTTPフォームベース認証の設定
FirePassからHP IceWall SSOへ認証問い合わせを行うためには、「マスターグループ設定」でリモートアクセス用の新しいマスターグループ設定を行います。
新しいマスターグループではHTTPフォームベースの認証を選択し、HP IceWall SSO固有のログイン電文を送るよう設定します。

設定内容

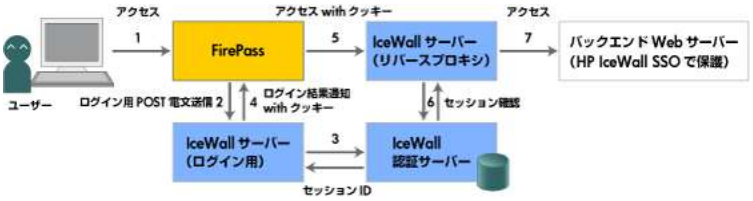
- 認証->マスターグループ設定画面」で新しいマスターグループを作成し、認証方式に「HTTPフォームベース」を選択します。
- 「HTTPのフォームベース認証画面」で必要なパラメーターを定義します。

＜FirePassのHTTPフォームベース認証設定・例（抜粋）＞

- フォームアクション：http://sso.icewall.hp.com/fw/dfw
- ユーザー名のフォームパラメーター：ACCOUNTUID
- パスワードのフォームパラメーター：PASSWORD
- Hiddenフォームパラメーターと値：HIDEURL=/login LOGIN=ICEWALL_LOGIN
- クライアントブラウザにcookieを渡すのをチェック：有効
- 成功したログオンの検知：特定のcookie が存在することによって
- Cookie名：IW_INFO

※「Webアプリケーションお気に入り設定画面」では、HP IceWall SSO経由で最初にアクセスさせたいURL（ダイナミックメニューポータル等）を適宜定義します。

HTTPフォームベース方式認証による連携フロー



1. ユーザーがFirePassにアクセスし、ユーザーIDとパスワードを送信します。
2. FirePassがIceWallサーバーのログイン用URLにログイン用のPOST電文を送信します。
3. IceWallサーバーが認証サーバーに認証要求をしてセッションIDを取得します。
4. IceWallサーバーがHP IceWall SSOのセッションクッキーを返信します。
5. IceWall経由のURLにHP IceWall SSOのセッションクッキーとともにアクセスします。
6. IceWallサーバーが認証サーバーにセッションを確認します。
7. IceWallサーバーがアクセスをバックエンドWebサーバーに中継します。

※この例ではログイン用とリバースプロキシの二つのIceWallサーバーを用意していますが、1つのIceWallサーバーで実現することも可能です。

おわりに

今回ご紹介した構成ではHP IceWall SSOのローカルデータベースのユーザー情報のみを利用してFirePassへのログインを行っており、ユーザー情報の一元管理を実現しています。
本ソリューションを発展させることでWebアクセス以外のリモートアクセスにもシングルサインオンやユーザー一元管理の範囲を広げることができます。

2009.7.17 日本ヒューレット・パッカード 日本ヒューレット・パッカード テクノロジーサービス統括本部 テクニカルコンサルタント 徳永 拓
協力：東京エレクトロンデバイス株式会社

関連技術レポート
≫ SSL VPNアプライアンスとの連携 F5ネットワークス社 FirePass（本レポート）
≫ SSL VPNアプライアンスとの連携 ジュニパーネットワークス社 Secure Access 2500