HP IceWall SSO

HP IceWall技術レポート：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

はじめに

社外からイントラネットのサーバ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。
今回は、ジュニパーネットワークス社Secure Access 2500との連携方法をご紹介します。

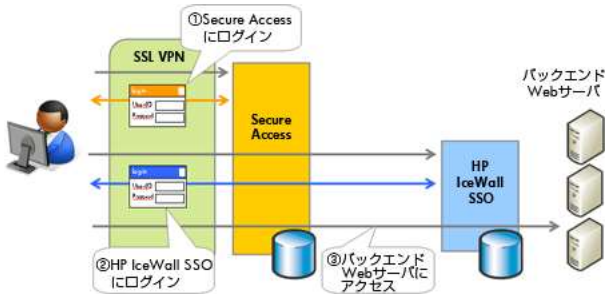
ジュニパーネットワークス社 Secure Access 2500

ジュニパーネットワークス社Secure Access 2500(以下 Secure Access)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。

Secure Access 2500とHP IceWall SSOの連携のメリット

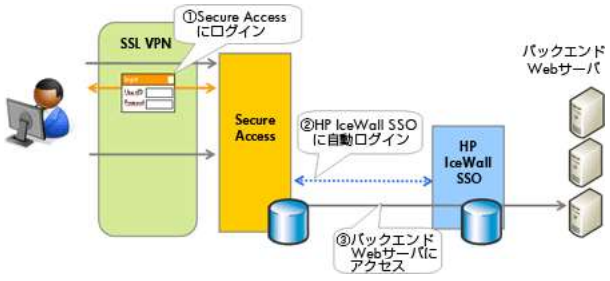
Secure Access 2500とHP IceWall SSOの認証を連携させない場合

ユーザは、Secure Accessに登録されたユーザID/パスワードを入力してSecure Access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ID/パスワードを入力してHP IceWall SSOにログインします。



Secure Access 2500とHP IceWall SSOの認証を連携させた場合

ユーザは、Secure Accessに登録されたユーザID/パスワードを入力してSecure Accessにログインします。
その後、ユーザがHP IceWall SSOのバックエンドWebサーバにアクセスする際に、Secure Accessが自動的にHP IceWall SSOのログイン電文を送信してログインします。
このためユーザから見ると、Secure AccessからHP IceWall SSOにシングルサインオンすることができます。



Secure Access 2500とHP IceWall SSOの連携方法

■ ユーザレポジトリ
Secure Accessのローカルデータベースと HP IceWall SSOの認証データベースに同一ユーザ名、同一パスワードでユーザをそれぞれ登録します。

- Secure Access
  - Secure Accessのユーザレポジトリとしてローカルデータベースを使用します。
  - 内部データベースには、Secure Accessにログインするためのユーザ/パスワードを登録します。
- 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/パスワードを登録します。

■ 接続形態
Secure AccessからHP IceWall SSOにアクセスするにはSecure AccessのWebリライティング機能を利用します。
Webリライティング機能では、Secure Accessがリバースプロキシの動作をすることでHTTPアクセスをイントラネットのWebサーバ（＝今回の場合はIceWallサーバ）に中継します。

■ リモートSSO機能
Secure AccessからHP IceWall SSOにシングルサインオンをするためにはSecure Accessのリモート SSO機能を利用します。
リモートSSO機能では、Webサーバにアクセスする前にWebサーバ固有のログイン電文を送ることができます。

設定内容

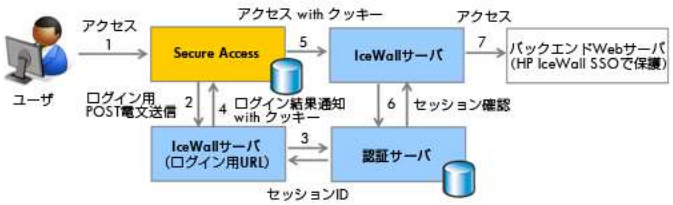
- HP IceWall SSO経由でバックエンドサーバにアクセスするためのURLを全てリモートSSOの対象として定義します。
- HP IceWall SSOのログイン後にユーザが誘導されるURLとして、ダイナミックメニューポータルを指定します。

＜Secure Accessのリモート SSOの定義・例（抜粋）＞

- Resource: http://sso.icewall.hp.com/fw/dfw/*
- Action: Perform the POST defined below
- POST to URL: http://sso.icewall.hp.com/fw/dfw
- POSTデータ:

User label	Name	Value	User modifiable
LOGIN	LOGIN	ICEWALL_LOGIN	Not modifiable
HIDEURL	HIDEURL	/DMP/dp/dmp	Not modifiable
Username	ACCOUNTUID	<USER>	Not modifiable
Password	PASSWORD	<PASSWORD>	Not modifiable

リモートSSO機能による連携フロー



1. Secure Accessで認証済のユーザがHP IceWall SSO経由のバックエンドWebサーバのURLにアクセスします。
2. Secure AccessがIceWallサーバのログイン用URLにログイン用のPOST電文を送信します。
3. IceWallサーバが認証サーバ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経由のダイナミックメニューポータルの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サーバが認証サーバにセッションを確認します。
7. IceWallサーバがアクセスをダイナミックメニューポータルに中継します。

おわりに

今回ご紹介した構成ではSecure Accessのローカルデータベースを利用していますが、Secure AccessではLDAPサーバ等の外部のレポジトリで認証することもできます。
Secure Accessの外部レポジトリとHP IceWall SSOの認証データベースのユーザを同期することで、ユーザ情報を一元管理することも可能となります。
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元管理の範囲を広げることができます。

2009.1.13 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 ソリューションアーキテクト山口 晃 /協力：ノックス株式会社

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