

Barracuda SSL VPN は標準 Web ブラウザを利用して、ファイル、イントラネット Web サイト、または、クライアント/サーバアプリケーションのような内部ネットワークリソースへセキュアなリモートアクセスを実現するアプライアンス製品です。一般的には、Barracuda SSL VPN を LAN 内部に配置するか、DMZ 内部に配置します。

1 はじめに

この資料は Barracuda SSL VPN の導入手順を纏めたものです。円滑に導入を行うために、作業を開始する前にこの手順書をお読み下さい。

Barracuda SSL VPN の導入に必要な物は以下のとおりです。

- Barracuda SSL VPN
- AC 電源ケーブル
- イーサネットケーブル
- VGA モニター (推奨)
- PS2 キーボード (推奨)

2 物理的な導入

Barracuda SSL VPN の物理的な導入を行います。

1. Barracuda SSL VPN を 19 インチラックに設置するか、その他の安定した場所に設置します。
2. お使いのスイッチから Barracuda SSL VPN の背面にあるイーサネットポートにイーサネットケーブルを接続します。
3. VGA モニター、PS2 キーボード、AC 電源ケーブルを Barracuda SSL VPN に接続します。注意：AC 電源ケーブルを接続すると、直後に電源が数秒間 ON になり、その後 OFF になります。これは本体が停電時に自動的に電源が ON の状態になるように設計されているためです。
4. フロントパネルにある電源スイッチ(Power Button)を押して、電源を入れます。



3 IP アドレスとネットワークの設定

モニターを接続している場合、まず始めにブートメニューが表示され、ブート後に管理者コンソールのログイン画面が表示されます。

1. 管理者の ID/PASSWORD を用いて管理者コンソールにログインします。

```

• Login:      admin      barracuda login: admin
• Password:  admin      password:
    
```

2. IP アドレス、サブネットマスク、デフォルトゲートウェイ、プライマリ DNS サーバ、セカンダリ DNS サーバを正しく設定します。

3. 設定した内容を保存します。

モニターとキーボードを用いずに、フロントパネルにあるリセットボタンを一定時間押し続けることで下記の IP アドレスを設定することもできます。

IP アドレス	リセットボタンを押し続ける秒数
192.168.200.200	5 秒
192.168.1.200	8 秒
10.1.1.200	12 秒

4 ファイアウォールのポートを開放

Barracuda SSL VPN をファイアウォールの背後に配置する場合、正しく動作するために、ファイアウォールで以下のポートを開放してください。

ポート	方向	TCP	UDP	用途
22	Out	Yes	No	リモート診断 (推奨) *
25	Out	Yes	No	警告メールとワンタイムパスワード通知
53	Out	Yes	Yes	ドメインネームサービス (DNS)
80	Out	Yes	No	ウィルス/ファームウェア更新
123	Out	No	Yes	ネットワークタイムプロトコル (NTP)
443	In/Out	Yes	No	SSL VPN アクセス用の HTTPS/SSL ポート
8000	In/Out	Yes	No	管理者インターフェースポート (HTTP) **
8443	In/Out	Yes	No	管理者インターフェースポート (HTTPS) **

* リモート診断を実施する場合に必要なになります。

** アプライアンス管理者インターフェースポート (8000/8443) はインターネットからアプライアンスを管理する場合のみ、開放します。

5 Barracuda SSL VPN の設定

Barracuda SSL VPN と同じネットワークに接続された PC から Web ブラウザにより以下の手順で設定を行います。:

1. ブラウザのアドレスバーで [http://](http://192.168.200.200:8000) に続いて「バラクーダの IP アドレス」、デフォルトの Web インターフェース http ポート「:8000」を入力します。バラクーダの IP アドレスが 192.168.200.200 の場合、<http://192.168.200.200:8000> と入力します。

2. 以下のログイン情報を利用して、Barracuda SSL VPN の Web 管理インターフェースにログインします。

Username: admin **Password:** admin

3. 「基本設定」の「IP 設定」画面を開き、以下の手順を行います。
 - IP アドレス、サブネットマスク、デフォルトゲートウェイが正しく設定されていることを確認します。
 - プライマリ、セカンダリ DNS サーバが正しく設定されていることを確認します。
 - ネットワーク上でプロキシサーバを利用している場合、プロキシサーバが正しく設定されていることを確認します。
4. 「変更保存」をクリックし、設定内容を保存します。

6 ファームウェアの更新

「高度な設定」の「ファームウェア更新」画面を開きます。利用可能な最新バージョンがダウンロード可能な状態であれば、以下の手順でシステムファームウェアの更新を実施します。:

1. インストールしたいファームウェアバージョンの隣にある「**今すぐダウンロード**」をクリックします。ダウンロードの進捗状況を確認したい場合には、「**更新**」をクリックします。ダウンロードが完了した場合には、「更新」の代わりに「**今すぐ適用**」が表示されます。
2. 「**今すぐ適用**」をクリックし、ファームウェアをインストールします。ファームウェアの適用が完了するには数分間かかります。ダウンロードや適用を実施している最中に、バラクーダの電源を切らないで下さい。バラクーダの故障の原因となります。
3. ファームウェアが適用されると **Barracuda SSL VPN** は自動的に再起動し、システムが起動した際には、ログイン画面が表示されます。
4. 再度ブラウザからログインし、リリースノートを参照することを推奨します。また、ファームウェアの更新により機能が追加されている場合がありますので、設定項目を確認することを推奨します。

7 管理者パスワードの変更

セキュリティ上、デフォルトのパスワードからよりセキュアな任意のパスワードに変更してください。パスワードの変更はブラウザからのみ実施できます。

1. 「**基本設定**」の「**管理**」画面で現在のパスワードと変更後のパスワードを入力
2. 「**パスワードの保存**」をクリック

8 製品登録

「**基本設定**」の「**ステータス**」画面でエネルギー充填サービスが有効になっているか確認してください。

1. 「エネルギー充填サービスステータス」で、エネルギー充填サービスが「有効」になっていることを確認して下さい。エネルギー充填サービスが有効になっていない場合、製品登録リンクをクリックしてバラクーダネットワークス製品登録ページで製品登録を完了してください。
2. **Barracuda SSL VPN** を再起動します。

9 SSL 通信を Barracuda SSL VPN に転送

Barracuda SSL VPN の機能を利用するためには、ポート 443 の HTTPS 通信をバラクーダに転送するような設定が必要です。一般的に、ファイアウォールで、SSL 通信を **Barracuda SSL VPN** へポートフォワーディングすることで可能となります。

注意: 企業ネットワークの外部から管理を行う場合、管理者 Web インターフェースポート(8000/8443)は同様のポートフォワーディング設定が必要となります。

10 Barracuda SSL VPN への接続確認

ファイアウォールに、SSL 通信を **Barracuda SSL VPN** に転送するように設定することで、SSL 接続が可能になります。

1. 接続確認のために、インターネット (LAN 内部ではない) から Web ブラウザでファイアウォールの外部 IP アドレスに SSL 通信を確立します。例えば、ファイアウォールの外部 IP アドレスが 192.168.1.1 の場合、ブラウザで <https://192.168.1.1> に接続します。
2. 信頼されていない SSL 証明書を受信すると、ブラウザの画面に警告メッセージが表示されます。警告を承諾し、ページを読み込みます。
3. **SSL VPN** のユーザインターフェースのログイン画面が表示されます。以下の管理者 ID/PASSWORD を用いてログインします。
 - Login: ssladmin
 - Password: ssladmin
4. ログインに成功すると、**SSL VPN** の管理者として管理インターフェースに直接繋がります。この段階でアカウントの作成、または、**Barracuda SSL VPN** のユーザに接続を許可するリソースの設定が可能となります。

11 追加セットアップ設定

インターネットからの接続を許可するために、**Barracuda SSL VPN** に基本的な設定を行います。以下の追加手順に関して、より詳しい情報が必要な場合は、管理者ガイドを参照して下さい。

- DNS サーバに、**Barracuda SSL VPN** 用のホスト名を登録します。
例: `sslvpn.company.com`
- このホスト名用の **Barracuda SSL VPN** の SSL 証明書をインストールします。ユーザは、組織に登録されている **Barracuda SSL VPN** に接続していることを証明することができます。
- 既存ユーザデータベースを **Barracuda SSL VPN** に統合します。正確に環境を統合するために、バラクーダは **Microsoft Active Directory** を含む複数のデータベースからユーザアカウントと認証情報を読み込むことができます。
- **SSL VPN** のユーザがリソースに接続できるように許可します。ポリシーベースアクセス制御フレームワークの使用の詳細については、管理者ガイドを参照して下さい。
- ネットワークに DMZ がある場合、**Barracuda SSL VPN** をそこに配置して、セキュリティを強化します。

以下のサイトにより管理者ガイドをダウンロードすることができます。

<http://www.barracuda.com/documentation>.