


AWS(EC2)でSoftEtherを使ってL2TP/IPsecなVPNを構築する (Mac)


EC2(/tags/EC2) 1042 SoftEther(/tags/SoftEther) 29 l2tp-ipsec-vpn(/tags/l2tp-ipsec-vpn) 9 VPN(/tags/VPN) 167 Mac(/tags/Mac) 4939

👍 176
いいね

💬 9
コメント

👍 いいね

 (/yaquawa) (/koginoadm) (/nanzono) (/H_Holon) (/iogii) (/Miruscon) (/veryshj123) (/fukuiii) (/kento-o) (/K_Yagi) ... (/showwin/items/92861057a8b62611444d/likers)

 showwin (/showwin) 2017年05月19日 21時52分に更新 🔁 (/showwin/items/92861057a8b62611444d/revisions) 9

📁 184ストック ...

SoftEther (<http://ja.softether.org/>)のVPNソフトがすごい！らしいので、EC2のAmazon Linuxで環境構築をしてみた。
2014年の頭にOSSになって、無償でつかえるようになったらしい。

[追記]

2016/04/17 最新版の v4.20-9608-rtm の情報に更新

2015/11/16 最新版の v4.18-9570-rtm の情報に更新

環境

サーバー側

- EC2 t2.micro Amazon Linux
- SoftEther VPN

クライアント側

- Mac OS X (10.9.5 or higher)
- iOS (8.1 or higher)
- Android, PC (動作未確認ですが、普通に動くはず)
- Macしか手元に無く、SoftEtherのWindows向けGUIソフトが使えない前提です。

その他の記事

- L2TP/IPsecではなくて、SoftEther標準のクライアントで接続する場合はここを見るといいかもしれません。
 - <http://qiita.com/ask/items/9ff1529d228ec093aa07> (<http://qiita.com/ask/items/9ff1529d228ec093aa07>)
- クライアントがLinuxの人はここを見るといいかもしれません。
 - <http://blog.memolib.com/memo/736> (<http://blog.memolib.com/memo/736>)
- クライアントがWindowsの人は、Windows向けのGUIツールを使った導入記事がたくさんあります。
 - 自分でググれ！
- 公式のドキュメント
 - <http://ja.softether.org/4-docs> (<http://ja.softether.org/4-docs>)

1. サーバー(EC2)にSoftEtherをインストール

基本的には公式ドキュメントのここ (<http://ja.softether.org/4-docs/1-manual/7/7.3>)に沿って行えば良いです。

```
1
2 # 以下すべてrootで行います
3 $ sudo su -
4
5 # make で必要
6 $ yum install -y gcc
7
8 # ソースコードを落としてきます。
9 $ wget http://jp.softether-download.com/files/softether/v4.20-9608-rtm-2016.04.17-tree/Linux/SoftEther_VPN_Server/64bit_-_Intel_x64_or_AMD64/sc
10
11 # 解凍する
12 $ tar -zxvf softether-vpnserver-v4.20-9608-rtm-2016.04.17-linux-x64-64bit.tar.gz
13
14 $ cd vpnserver
15
16 # ビルド
17 $ make
18
```

make をした後に、ダラダラと文字が流れてきて、ライセンスに同意しますか？と聞いてくるので、すべて 1 と回答する。

作成したvpnserverを /usr/local に置く。

```
1
2 $ cd
3 $ mv vpnserver /usr/local
```

ファイルの権限を変更する。

```
1
2 $ cd /usr/local/vpnserver/
3 $ chmod 600 *
4 $ chmod 700 vpncmd
5 $ chmod 700 vpnserver
```

SoftEtherのコマンドラインを使って、正しく設定ができているか確認する。

```
1
2 $ ./vpncmd
```

どのモードを使うか聞いてくるので、3 を入力して

```
1
2 VPN Tools> check
```

とコマンドを入力する。

6つぐらいのテストをパスすれば、とりあえずここまではOK。

```
1
2 VPN Tools> exit
```

一旦終了。

2. スタートアップスクリプトへの登録

バックグラウンドで常に行わせるために、デーモンプロセスとして登録する。
/etc/init.d/vpnserver に以下を書き込む。

```
1 #!/bin/sh
2 # chkconfig: 2345 99 01
3 # description: SoftEther VPN Server
4 DAEMON=/usr/local/vpnserver/vpnserver
5 LOCK=/var/lock/subsys/vpnserver
6 test -x $DAEMON || exit 0
7 case "$1" in
8 start)
9 $DAEMON start
10 touch $LOCK
11 ;;
12 stop)
13 $DAEMON stop
14 rm $LOCK
15 ;;
16 restart)
17 $DAEMON stop
18 sleep 3
19 $DAEMON start
20 ;;
21 *)
22 echo "Usage: $0 {start|stop|restart}"
23 exit 1
24 esac
25 exit 0
```

root以外のユーザが変更できないように、ファイルの権限を変更する。

```
1
2 $ chmod 755 /etc/init.d/vpnserver
```

サーバーを再起動した時にも自動的にVPNサーバーが起動するように設定

```
1
2 $ /sbin/chkconfig --add vpnserver
```

動くかどうか試してみる

```
1 $ service vpnserver start
2 > The SoftEther VPN Server service has been started.
```

となればOK。

3.クライアントのアカウント作成

既存の記事はここからWindowsのGUIソフトを使うものばかりだったので、サーバー側でCUIで設定する方法を書く。

コマンドラインを起動する。

```
1
2 $ cd /usr/local/vpnserver/
3 $ ./vpncmd
```

今回はサーバーの設定をするので、1のモードを選択。

接続先のホスト名 と 仮想HUB名 を聞かれるけど、空白のままEnterを2回押せば良い。

このコマンドラインで使えるコマンドはHELP と入力すると、全部見れる。全部で205個のコマンドがあるらしい。
(ちなみに、コマンドの大文字小文字は関係なく、コマンドのスペルを少し間違えても推測して訂正してくれてすごい。)

仮想HUBの作成

仮想HUBが何なのかよく理解できていないけど、感覚的には、ユーザは仮想HUBに属していて、VPNを繋ぐ時の認証などはそこに所属する仮想HUBが担当するものらしい。

学校のクラスみたいなものを想像すればよいのかな。

とりあえず

```
1 VPN Server> HubList
```

という仮想Hubの一覧を見るコマンドを打てみると、 DEFAULT という仮想HUBが既に作られているのが分かる。
でも、やっぱり自分で作ったものがあると嬉しいので、 example という名前の仮想HUBを作ってみる。

```
1 VPN Server> HubCreate
2 HubCreate コマンド - 新しい仮想 HUB の作成
3 作成する仮想 HUB の名前: example
4
5 パスワードを入力してください。キャンセルするには Ctrl+D キーを押してください。
6
7 パスワード:*****
8 確認入力 :*****
9
10 コマンドは正常に終了しました。
```

となればOK。

ユーザの作成

既存のユーザがいるのかなと調べてみる

```
1 VPN Server> UserList
```

とすると

```
1 UserList コマンド - ユーザー一覧の取得
2 このコマンドを実行する前に、Hub コマンドで管理対象の仮想 HUB を選択してください。
```

と怒られてしまう。

管理対象の仮想HUBを指定しないといけないようなので

```
1 VPN Server> HUB example
```

として、仮想HUB example を指定する。

```
1 VPN Server/example> UserList
```

とすると、まだだれもユーザがいらないようなので、新しく hoge さんを作成する。

```
1 VPN Server/example> UserCreate
2 UserCreate コマンド - ユーザーの作成
3 ユーザー名: hoge
4
5 参加するグループ名: #option 空白EnterでOK
6
7 ユーザーの本名: #option 空白EnterでOK
8
9 ユーザーの説明: #option 空白EnterでOK
10
11 コマンドは正常に終了しました。
```

となればOK。

認証方法は5種類ぐらい用意されているらしいけど、今回はパスワード認証を選ぶことにする。

```
1 VPN Server/example> UserPasswordSet
2 UserPasswordSet コマンド - ユーザーの認証方法をパスワード認証に設定しパスワードを設定
3 ユーザー名: hoge
4
5 パスワードを入力してください。キャンセルするには Ctrl+D キーを押してください。
6
7 パスワード: *****
8 確認入力 : *****
9
10
11 コマンドは正常に終了しました。
```

となればOK。

これでユーザ作成は完成。

簡単！！！！

4. L2TP/IPsecなVPNにする

MacやiOSなど(PC,Androidも含めて)では標準でL2TP/IPsecでVPN接続できるので、それに対応できるようにする。
公式ドキュメントでは以下の辺りを参考にすると良いと思う。

- VPN Server 側での L2TP/IPsec 機能の有効化方法 (http://ja.softether.org/4-docs/2-howto/L2TP_IPsec_Setup_Guide/1)
- 6.3.69 "IPsecEnable": IPsec VPN サーバー機能の有効化 / 無効化 (http://ja.softether.org/4-docs/1-manual/6/6.3#6.3.69_22IPsecEnable.22:_IPsec_VPN_.E3.82.B5.E3.83.BC.E3.83.90.E3.83.BC.E6.A9.9F.E8.83.BD.E3.81.AE.E6.9C.89.E5.8A.B9.E5.8C.96_2F_.E7.84.A1.E5.8A.B9.E5.8C.96)

引き続き、コマンドラインで作業を続ける。

IPsecEnable とコマンドを入力すると、いくつか設定の値を聞かれるので、以下のように答える。

```
1 VPN Server/example> IPsecEnable
2 IPsecEnable コマンド - IPsec VPN サーバー機能の有効化 / 無効化
3 L2TP over IPsec サーバー機能を有効 (yes / no): yes
4
5 Raw L2TP サーバー機能を有効 (yes / no): no
6
7 EtherIP / L2TPv3 over IPsec サーバー機能を有効 (yes / no): no
8
9 IPsec 事前共有鍵の文字列 (9 文字以下を推奨): *****
10
11 VPN 接続時に仮想 HUB 名が省略された場合のデフォルト仮想 HUB 名: example
12
13 コマンドは正常に終了しました。
```

これだけで、L2TP/IPsec で接続できるようになる。すごい。

L2TP/IPsec で繋ぐには、UDPのポートをいくつか開けないといけないので、AWSのセキュリティグループで以下のものを開けておく

- UDP 500
- UDP 4500
- ~~UDP 1701~~ ←不要です

【追記】

UDP 1701 は開放不要とのコメント (<http://qiita.com/showwin/items/92861057a8b62611444d#comment-a4efdae3a6c09f3da8a2>)を頂きました。ありがとうございます！

5. ぼくがめちゃくちゃハマったところ

「仮想 NAT および DHCP サーバー機能 (SecureNAT 機能) の有効化」をする必要があった。
だけど、実はこれが何なのかよく分かっていない。勉強不足。。

これもコマンドラインで有効化する。

```
1 VPN Server/example> SecureNatEnable
```

これを有効化しないと、クライアントから接続した時に「PPPサーバーとの接続が確立ができません」みたいなエラーが出る。
SoftEtherのログインログを見てみると、ちゃんとログイン回数は増えていたので、認証は通るけど、そのあとVPNが正しく構築されないという状況らしい。

これで5時間ぐらいハマった。

6. めでたくMacからVPN接続する

いつものシステム環境設定からVPN繋ぐやつ。

よくわからない人は公式ドキュメントのここ (http://ja.softether.org/4-docs/2-howto/L2TP_IPsec_Setup_Guide/5)を見てください。
iOSの場合はこっち (http://ja.softether.org/4-docs/2-howto/L2TP_IPsec_Setup_Guide/2)。

ちょっと注意すべきなのはアカウント名が [ユーザ名]@[仮想HUB名] になること。

```
1 VPN Server/example> IPsecEnable
2 (略)
3 VPN 接続時に仮想 HUB 名が省略された場合のデフォルト仮想 HUB 名: example
```

に指定した仮想HUB(上の例では example)に所属する場合はアカウント名から @[仮想HUB名] を除いた [ユーザ名] だけでもログインできます。

7. ついでに宣伝

回線状況が悪いところでネットをしていて、ブツブツVPNが切れると何回も繋ぎ直したりしてイライラしますよね。
そんなあなたのために、自動でVPNを繋ぎ直してくれるMac向けのアプリケーションを作ったりするので、興味ある人はどうぞ。
ダウンロード: <https://github.com/showwin/FeVPN/releases> (<https://github.com/showwin/FeVPN/releases>)
ソースコード: <https://github.com/showwin/FeVPN> (<https://github.com/showwin/FeVPN>)

Tweet0

G+

Like 0

93

 (/showwin)

showwin (/showwin)
255 Contribution

フォロー

人気の投稿


- AWS(EC2)でSoftEtherを使ってL2TP/IPsecなVPNを構築する (Mac) (/showwin/items/92861057a8b62611444d)
- CopybaraでJSを使ったテストは save_screenshot が便利 (/showwin/items/cf047bfd9a3c08781bf7)
- Amazon Linuxにmysql2を入れようとしたらエラーがでる (/showwin/items/e069bbba9c87a6c7d91c)
- MySQLでdatabase内のすべてのカラム名を取得する (/showwin/items/0ac4abca8a1401213fa1)
- Rails で Session Store が使えないと思ったら rails-api が原因だった (/showwin/items/fa514fe45c26eae22a29)

- 環境
- サーバー側
 - クライアント側

- その他の記事
1. サーバー(EC2)にSoftEtherをインストール
 2. スタートアップスクリプトへの登録
 3. クライアントのアカウント作成
 - 仮想HUBの作成
 - ユーザの作成
 4. L2TP/IPsecなVPNにする
 5. ぼくがめちゃくちゃハマったところ
 6. めでたくMacからVPN接続する
 7. ついでに宣伝

いいね

176





(/miseyu) (/kasumani) (/heliac2000) (/k-shogo) (/magifd2) (/turtle2005) (/syano) (/morozumi_h) (/miramba_) (/white_aspara25)

... (/showwin/items/92861057a8b62611444d/likers)

184ストック 編集リクエスト (/drafts/92861057a8b62611444d/edit) ...

🔗 この記事は以下の記事からリンクされています


 **SoftEther vpnserver (接続できた)** (/tukiyo3/items/3a123db45404d30d7a07#_reference-e7453502673c6d6959ac) からリンク 2年以上前

 (**kawanet (/kawanet)**) 188 contribution

2015-07-22 00:46

いいね1

ソフトイーサのドキュメントは膨大なので、まとめていただき、大変助かりました。ありがとうございます。
私は VPN 経由で外部に接続する環境を構築したかったので、
上記記載の IPsecEnable と SecureNatEnable に加えて、
NatEnable と DHCPEnable も必要でした。

 (**polikeiji (/polikeiji)**) 371 contribution

2015-10-08 07:52

いいね0

ちょうど、SecureNatEnableで、ぼくもはまってて、本当に助かりました！

 (/showwin)

showwin (/showwin)
255 contribution

2015-10-08 07:54

いいね0

ちょうど、SecureNatEnableで、ぼくもはまって、本当に助かりました！

お役に立てて良かったです！



nori3tsu (/nori3tsu)

(/nori3tsu) 402 contribution

2015-12-16 18:38

いいね

2

本記事の内容だとIPsecなしのL2TPは扱わないので、UDPのポートは500,4500のみ開くほうが安心ですね。

引用: VPN Server 側での L2TP/IPsec 機能の有効化方法 - SoftEther VPN プロジェクト (https://ja.softether.org/4-docs/2-howto/L2TP_IPsec_Setup_Guide/1)

L2TP over IPsec、EtherIP over IPsec を使用する場合
UDP ポート 500、4500
L2TP (IPsec なし) を使用する場合
UDP ポート 1701



showwin (/showwin)

(/showwin) 255 contribution

2015-12-17 07:03

いいね

0

ご指摘ありがとうございます！

引用までして頂いてありがとうございました。本文の内容を修正しておきました。



impreza1006 (/impreza1006)

(/impreza1006) 1 contribution

2016-05-11 16:30

いいね

0

AWSのVPC環境に本VPNサーバーを立てると、PCクライアントからの接続後はVPC内の別のサーバー（プライベートな口しかもっていないサーバー）へ疎通できることが必須となるのですが、その方法は検証されたりしていませんか？SoftEther VPNの「tap」という機能を使って実現できるみたいなのですが今一仕様がわからず。もし、お時間があれば記事にして頂きたい。AWSのプロミスキャスモードが色々影響しているみたいです。



showwin (/showwin)

(/showwin) 255 contribution

2016-05-11 18:30

いいね

0

@impreza1006 (/impreza1006) さん

すみません、検証していないですね 🙇

やりたいことが少しズレているかもしれませんが、以下の記事が参考になったりしますでしょうか。

<https://blog.cloudpack.jp/2014/10/27/aws-secure-private-env-with-oss-softether-nat/> (<https://blog.cloudpack.jp/2014/10/27/aws-secure-private-env-with-oss-softether-nat/>)



impreza1006 (/impreza1006)

(/impreza1006) 1 contribution

2016-05-12 18:03

いいね

0

既にリンク先の通りに設定したのですが、pingすら飛ばない状態でして。。もう少し色々試してみます。ありがとうございました！



impreza1006 (/impreza1006)

(/impreza1006) 1 contribution

2016-05-16 18:10

いいね

1

自己解決しました。VPN接続用にPrivateセグメントのNICを1枚追加して構成していたのですがどうやらそれがいけなかったみたいです。デフォルトで構成されるグローバルIP（Public用のIPセグメント）を持っているNIC1枚で本記事の通り構成し、追加でローカルブリッジの設定でそのNICを指定したら、Privateセグメントのサーバーとも通信できました。ですので、ローカルブリッジでTAPデバイスは使用せず、EC2のNICの設定にあるSource/Distチェックも無効化せずに通信できました。上記セグメントに属しているNICであればVPN接続用に1枚追加して、それをローカルブリッジで指定しても動作しました。

理由は不明ですが、他の方の参考になれば。。

