OpenVPN とプライベートクラウドの活用

西見　英里子　(指導教員: 金子 晃)

1　はじめに

ブロードバンドやモバイル向けデータ通信、公衆無線 LAN などを利用して、インターネット経由で会社や自宅の LAN にアクセスしたり、離れている 2 つの拠点をインターネットで接続したいと考える人も多いだろう。暗号技術を利用し、盗聴や改ざんのリスクを回避した仮想プライベートネットワーク（VPN:Virtual Private Network) を構築することで、簡単で安全な通信を可能にする。また、実際に eucalyptus というオープンソースを用いて、プライベートクラウドを構築し活用を試みる。

2　VPN/OpenVPN とは

VPN とは暗号技術を利用してパブリックなネットワーク上にトンネルのようなものを作成し、そのネットワークを、プライベートなネットワークとして利用したものである。通信路を暗号化しているため、通信を盗聴されたり、データを改ざんされる危険性がなく、ファイルサーバのようにインターネット上では提供しにくいサービスであっても、提供が可能となる。また、OpenVPN は、米 OpenVPN Technologies 社が開発している SSL-VPN ソフトウェアで、レイヤー 2 またはレイヤー 3 のパケットを SSL/TLS でカプセル化するという特徴がある。これにより、TCP だけでなく IP についても暗号化が可能になる。

3　接続形態

クライアントとサーバー間の接続形態は、「ルーティング接続」と「ブリッジ接続」の二種類がある。ルーティング接続は、仮想トンネルネットワークを経由して会社や自宅の LAN に接続する方法で、クライアントは会社や自宅の LAN と異なるネットワークにつながっているため、ルーティングを設定することで相互に通信できるようになっている。ルーティング接続のメリットは、クライアントと接続先 LAN のネットワークが異なるので、大規模化とアクセス制御をしやすいことである。ブリッジ接続は、仮想インタフェース（TAP インタフェース）を経由して会社や自宅の LAN と接続する方法で、LAN と同じ IP アドレス体系を、クライアントの TAP インタフェースに割り当てる。同一ネットワークにつながるため、クライアントはルーティングを意識する必要がなく、メリットは、ブロードキャストを使うアプリケーションを利用できることで、Samba や Windows ファイルサーバー、NetBIOS のブラウジング機能を利用したい場合に向いている。また、IP 以外のプロトコルを使えるため、個人や小規模ではブリッジ接続の方が使いやすい。

4　OpenVPN の構築の手順

(1) 導入

クライアントとサーバーのいずれにも、OpenVPN をインストールする。

(2) 秘密鍵と証明書の生成

OpenVPN は「公開鍵基盤」(PKI) がベースになっており、導入に当たり公開鍵や秘密鍵を生成したり、サーバー証明書を発行したりする必要があるため、認証局 (CA) を用意する。

(3)DH パラメータの生成

DH(Diffie-Hellman) パラメータを生成する。

(4) 秘密鍵と証明書の配置

ここまでに生成した各種ファイルを図 1 で示したように配置する。

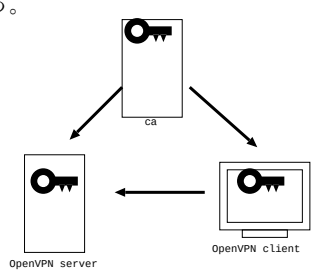

図 1．PKI の構成と秘密鍵、証明書の配置

5　OpenVPN の設定

上の図 1 で示した構成を想定して作業を進める。

(a) ルータの設定

ブロードバンドルーターが OpenVPN クライアントからのアクセス要求を OpenVPN サーバーに転送できるように、ポートフォワーディングを設定する。

(b)OpenVPN サーバーの設定。

今回はブリッジ接続を使うため、始めにブリッジインタフェースを生成する。次に、ファイアウォールの設定を行う。この時ポートはデフォルトの UDP の 1194 番ポートを利用する。設定ファイルを作成、編集し、OpenVPN サービスを起動する。

(c)OpenVPN クライアントの設定。

最後にクライアントを設定する。設定ファイルの作成、編集を行い、OpenVPN クライアントを起動する。エラーが出ずに、強制終了しなければ正常に起動していることになる。

6　プライベートクラウドとは

クラウドとは、コンピュータ機器類とウェブサービスの集合である。ユーザの要求に応じて一時的にサービスを提供し、終了と同時に返却させる。ユーザからは、どこのコンピュータを使っているのかがわからないので、「クラウド」と呼ばれる。VM（virtual machines）技術の進歩により、効率的なクラウドサービスの実現が可能になった。

プライベートクラウドとは、ユーザ企業などが閉じたネットワークで使うクラウドのことで、Amazon EC2 などのパブリッククラウドと異なり、データを外に置かない分、セキュリティが高いと言える。また、サーバを集約してリソースを効率的に使えるため、コストを削減できる効果も期待できる。今回は Nikkei Linux に収録されている Ubuntu Enterprise Cloud (UEC) という、Eucalyptus をベースに開発されたパッケージを使ってプライベートクラウドを作ってみた。これと平行して、本部サイトから Eucalyptus のソースをダウ

ンロード、メイクしてみた。また、実際にこれらの活用を試みた。

7 eucalyptus とは

Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems（プログラムと役に立つシステムをつなぐための、公共性の高い、実用的なコンピューティング・アーキテクチャ）は、「エラスティック」（汎用的）、「ユーティリティ」（公共的）、「クラウド」といったコンピュータの使用環境を実装するためのコンピューティング・クラスタ環境や、ワークステーション・ファームで使うことが出来る、オープンソースのインフラストラクチャである。現時点における Eucalyptus のインターフェースは Amazon.com が提供する EC2 と互換性があり、インフラストラクチャはその他のクライアント型のインターフェースが利用可能となるように設計されている。更に、Eucalyptus はインストールやメンテナンスを簡単に行えるよう、一般的な既存の Linux のツールと同じように実装されているほか、基本的なウェブサービス技術を利用している。

また、eucalyptus は以下の特徴を持っている。

* Amazon EC2・S3 との互換インターフェース（いずれもウェブサービスと Query/REST インターフェースです）

* 簡単なインストールと設定

* 殆どの Linux ディストリビューションのサポート（ソースやバイナリパッケージの提供）

* WS-security プロトコルを使った SOAP 通信で、内部の通信をセキュア（安全）なものにする

* オーバレイ機能を必要としている Linux 環境向けの最低限の修正

* システム管理とユーザ管理を行うためのクラウド・アドミニストレータ・ツールズ (Cloud Administrator tools)

* 1 つのクラウド環境に複数のクラスタ環境（プライベートな内部ネットワークアドレスを使うなど）を構築する能力

8 UEC の大まかな仕組み

Eucalyptus は以下の役割の異なる複数のコンピュータから構成される。

・インスタンスを稼働させるコンピュータ群 (Node)

・それらのクラスターを管理するコンピュータ (Cluster)

・ユーザからのリクエストを受け付けるコンピュータ

・ストレージを管理するコンピュータ

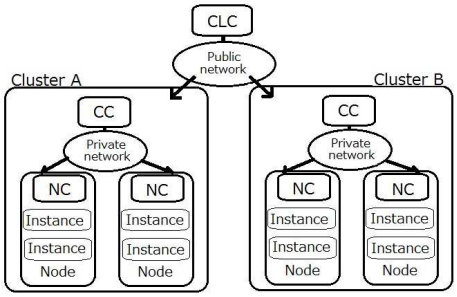

図 2. Eucalyptus(UEC) の基本構成

インスタンスは、停止または再起動を行うと設定情報やデータが消失するため、それらの情報を保持するために仮想ボリューム (EBS 機能) を使う。

UEC では、これらの複数のサービスを同一マシンにまとめることにより、Node と Cluster の最小２台で構築できるようになっている。

9 UEC のインストールと起動

7 で述べたように、空き容量が 20GB ある Cluster 用マシンと Node 用マシンを用意する。ここで、Node となるマシンには、Intel の CPU の仮想化支援機構「IntelVT」を用意しておく。

(1)UEC の Cluster マシンへの導入

(2)UEC の Node マシンへの導入

この時、Cluster が起動し、ネットワークに接続されている状態で Node をインストールする。

(3)Node の登録

Node の登録は以下の手順で行う。

(3-1)Cluster の状況確認

Cluster の情報を参照する。Cluster の名前と IP アドレス、スペックが表示される。

(3-2) 仮想マシンイメージの登録

インスタンスの基となる仮想マシンのイメージを登録する。

(3-3) キーペアの登録

RSA のキーペアを登録する。イメージには SSH でログインするため、キーが必要となる。Eucalyptus がパブリックキーを保持して、インスタンス作成時に root ログイン用にパブリックキーを埋め込み、プライベートキーを持つユーザだけがログインできるセキュアな仕組みを作る。但し、キーペアの登録を複数回実施すると、サーバ側の情報が更新されないため、サーバ側のパブリックキーとローカルにあるプライベートキーの整合性がとれなくなってしまう。そのため、再度キーペアを登録する場合は、一度キーペアを削除する。

(3-4) インスタンスの起動

ssh でログインし、インスタンスを起動する。

(4) 外付けディスク「EBS」を使う

(3) でインスタンスにログインするが、インスタンスは物理マシンや仮想マシンとは異なり、停止するとすべての変更が失われてしまう。そこで、データを永続的に保持するために、EBS を使用する。

10 今後の課題と目標

OpenVPN やプライベートクラウドを実際に活用し、SaaS(Software as a Service) のサーバーを構築し、顧客にだけ、ある一定以上の内部を公開できるような仕組みを作り、商売を試みる。例えば、大学の授業を配信し、質問をデータベースと計算サーバを活用して自動応答する、等が考えられる。(macsyme,scilab 等の GPL の Open ソフトを利用する。)

参考文献

[1] Eucalyptus のサイト. `http://open.eucalyptus.com`

[2] 田中毅行、西村大介、日経 Linux 2010.4 月号、pp.71–82.

[3] 滝澤隆史、日経Linux 2010.8月号、pp.157–162.