MACアドレスによるネットワーク利用者認証システム OpengateMの負荷テスト

中林淳一 * 渡辺義明 *
(*佐賀大学大学院 工学系研究科 知能情報システム学専攻)

1 はじめに

佐賀大学ではインターネット利用に対する利用者の認証・記録を行う Opengate[1] が運用されている。Opengate は GUI として Web ブラウザを利用しており、ID とパスワードを入力することにより認証を行う。しかし、近年端末の多様化に伴い一部対応できないものが出てきた。そこで、MAC アドレスを用い認証処理を行う OpengateM[2] を提案・開発している。

本システムは、多数クライアントからのアクセスに対応できることが求められる。そこで、クライアントとゲートウェイ、サーバを 1Gbps ネットワークでつないだテスト環境を構築し、処理能力やハードウェア負荷の面から評価を行った。

2 認証方式

MAC アドレス認証は、様々な端末との互換性が高い、利用者端末側での特別な設定が不要などの利点がある。しかし、管理負担の増加や機器への登録数の制限などの問題により、多数の利用者がある環境における運用に向かない。そこで OpengateM は、ネットワークの利用開始時にパケット通過ルールをファイアウォール (FW) に登録し、終了時にルールを削除する手法を採用した。また、利用記録が取れる、データベース (DB) によるユーザ情報の集中管理が可能などの特徴がある。MAC アドレス偽装には、利用ログ提示による定期的な利用状況の確認や登録 MAC アドレスの利用期間の制限により対応する。

3 システムの構成と動作

OpengateM は、MAC アドレス認証を行うデーモンプロセス、パケットの通信を制御する FW、ユーザデータと利用記録を保持する管理 DB およびその管理システムからなる。MAC アドレスの取得には、libpcap によるパケットキャプチャ方式を用いる。

ユーザが端末からネットワークへアクセスすると、デーモンプロセスが通信パケットをキャプチャする。もし、パケットの送信元アドレスがキャッシュに存在すればチェック済みなので無視する。存在しない場合、DB で MAC アドレスが登録済みか確認する。登録済みであれば、FW に開放ルールを追加し、ネットワーク利用を可能にする。一定時間その端末からの利用がない場合は、FW から開放ルールを削除する。また、開放閉鎖時にログの記録を行う。

4 負荷テスト

OpengateM は、運用において多数の端末によるアクセスが予想される。そこで、サーバ (CPU:3.40GHz, Memory:1GB) とゲートウェイ (CPU:3.00GHz Core 2 Duo, Memory:4GB)、クライアント (CPU:3.40GHz, Memory:2GB) を 1Gbps ネットで接続し、負荷テストを行った。

デーモンプロセスにおける各種処理時間を計測したところ、キャッシュチェックに約 1μ 秒、DB アクセスおよびその他雑多に約 10m 秒という結果だった。今回、キャッシュの保持時間を 30 分と設定しており、ほとんどのパケットは μ 秒オーダで処理されると考える。また、サーバからクライアントへファイルダウンロードを行ったところ、1Gbps ネットワークの限界と考えられる 500Mbps 程度の速度を維持できた。この際、ゲートウェイマシンの CPU 負荷は最大で 60%程度であった。さらにディスクアクセスは、転送バイト数:0.02MB/s と busy 状態になることはなかった。以上から、最大流量においてハードウェア負荷に問題はないと考える。

次に、送信元 MAC アドレスをランダムに変化させながらパケットを送り付けるプログラムを作成して、多数端末の同時アクセスの模擬試験を行った。約 19000 パケット/秒の送信を行ったところ、プログラム開始時に新規アドレス確認の DB アクセスが集中して、パケットのキャプチャ漏れが発生した。30 分間のキャプチャ漏れ発生率は、1000 台では 1%未満であるが、1 万台では 10%、10 万台では 73%程度であった。図 1 に示す通り認証時にかかる CPU 負荷の変化から 1000 台程度であれば、すぐに処理し終えていることが確認できる。また、10 万台の同時アクセスであってもキャッシュ保持時間以内にはほぼ処理出来ている。さらに、極端に端末数を増やした状態で十数時間連続アクセスしても、マシンやデーモンプロセスが停止することはなかった。アクセスが集中している際、別端末からのアクセスが通りにくい場合があるが、数分程度繰り返しアクセスすればいずれ処理されることが確認できており、今回は許容範囲とする。

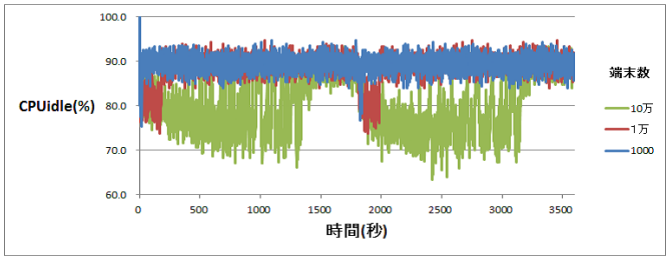

図 1: アクセス端末数毎の CPUidle 時間経過

なお、処理時間を短縮するには、キャッシュ上に全端末の情報を長時間保持すれば良い。しかし、以下の理由からこの方法は選択しない。まず、情報更新時のサービス連携が複雑になる。さらに高速化を行うと総当たり攻撃により、許容するアドレスの探索が短時間で出来てしまう。さらに本認証システムは、不正アクセス防止のために小さいサブネットに分割した運用が望ましく、一つのゲートウェイに膨大な端末数を想定しなくて良い。

5 まとめ

負荷テストの結果、1Gbps ネットワークにおいて 1000 台程度の端末による同時アクセスが生じても、十分対応できることが確認できた。

参考文献

[1] 渡辺義明 他, "Opengate", http://www.cc.saga-u.ac.jp/opengate/
[2] 渡辺義明 他, "OpengateM", http://www.cc.saga-u.ac.jp/opengate/opengatem/