

ファイアーウォール設定の検査手法

株式会社 山武

三島 崇
Takashi Mishima

株式会社 山武

佐内 大司
Daiji Sanai

キーワード

ファイアーウォール, インターネット, セキュリティホール

近年, 社会のネットワーク化が加速し, 企業のネットワークや産業用ネットワーク, 家庭などがインターネットによってシームレスに接続され始めた。そして, これらのネットワークを保護するための防護壁として, ファイアーウォールを設置することが一般的になっている。しかし, ファイアーウォールはセキュリティポリシーに則って正しい設定をしなければ防護壁の役をなさない。しかも, ファイアーウォールが正しく設定されているか確かめることは簡単ではない。

われわれは, ファイアーウォールの設定を検査するためのソフトウェア「ファイアーウォールチェッカー」を開発したので, その概要について解説する。

Inspection Techniques for Firewall Setting

In recent years, the need of computer networking has been drastically increasing. Business, industries and households are making connections to each other. In order to avoid malicious users from gaining access to precious data, it has become common practice to establish firewalls. However, a firewall does not serve as a shield unless it is configured appropriately according to a security policy. In addition, it is even more difficult to ascertain whether the security policy is appropriate or not. "Fire Wall Checker" is a piece of software we developed, which can inspect a firewall's settings. This paper outline its functionalities.

1. はじめに

社会のネットワーク化が加速している。企業活動を円滑にすすめていくためにE-Mailやウェブによる情報交換や情報収集はビジネス上, 不可欠なものとなり, 企業のネットワークは何らかの形でインターネットに接続する必要がある。一方, インターネットに接続することによって, 企業内のネットワークはインターネット上のクラッカーの標的になるリスクが発生する。このことは, インターネットの普及の比較的早い段階から問題とされており, 対策としてファイアーウォールというインターネットからの攻撃を防ぐ防護壁を設置することが一般的になっている。

インターネットテクノロジーは, 企業内ネットワークや産業用ネットワークなどにも採用され, それぞれシームレスな接続をはじめた。そして, ファイアーウォールはインターネットの防護壁として使われるだけでなく, 企業内

部門, テナント, 工場, 家庭など多くの場所で使われるようになってきたのである。

ファイアーウォールはソフトウェアによる防護壁であり, 物理的な防護壁ではない。つまり, 設置すれば役割を果たすものではない。ファイアーウォールが正しく防護壁として働くためには, セキュリティポリシーを実現するための適切なルールをファイアーウォールに設定しなければならない。もし誤った設定を行ってしまうと, ファイアーウォールは防護壁ではなくセキュリティホールとして働いてしまうことになる。つまり, ファイアーウォールはルールの設定が正しい場合にはじめて機能するのである。

われわれは, このファイアーウォールのルール設定が正しく行われているかを検査するためのソフトウェア「ファイアーウォールチェッカー」を開発したので, その概要について解説する。

2. ファイアウォール設定の問題点

2.1 わかりにくい設定

ファイアウォールのポリシー設定は難解である。個々のパケットごとに細かくルールを設定する必要があるが、この方法が人の思考方式に沿っていないことがひとつの原因としてあげられる。また、全体としてどのような設定に仕上がっているかを確認することが難しく、ファイアウォールの全体の問題点などが見えにくい。

2.2 誤ったデバッグ方法

ファイアウォールの設定が難しいためにその設定には誤りが多く発生するが、これらのデバッグは最終的にフィールドで行われることが多い。しかし、この方法が問題である。

ファイアウォールを通過すべきパケットが通過せずに拒否された場合、ユーザーは必要な業務を行えないので、ユーザーからクレームが発生する。そして、この設定ミスは修正されるであろう。しかし、通過してはいけないパケットが通過してしまっている場合、業務に支障がないのでどこからもクレームは発生しない。つまり、この設定ミスには誰も気が付かないのである。このような方法でファイアウォールがデバッグされた結果、設定ミスによるセキュリティホールはそのまま残り続けてしまうのである。

2.3 不可能な完全チェック

ファイアウォールの完全チェックを行うためには、利用可能なすべてのノードまたはネットワークからのパケット通過試験を行い、検査パケットがポリシー通りに通過したか、また拒否されたかを検査する必要がある。しかし、この検査パケットの数は天文学的な数字になり、事実上全パケットによる検査は不可能である。さらに、ファイアウォールの両側には、多階層の複雑なネットワークが物理的に離れて（東京 - 大阪など）存在していて、実際のパケットによる検査を行うことは難しい。結果として、「必要なパケットが通過していれば良い」という指針の検査に留まってしまうことが多いのである。

このように、ファイアウォールは導入されているが、それらの設定は検査されていないことが多い。これは、ファイアウォールの導入意義に相反する実態である。

3. ファイアウォールルールの検査手法

われわれは、このファイアウォールのポリシー設定を検査する方法について研究した。そして、2つの手法を考案し検討を行った。

3.1 シミュレータによる検査

ファイアウォールのパケット通過シミュレータソフトを作成して検査を行う（図.1）。

このシミュレータに検査対象のファイアウォールに設定してあるルール設定を適用して、検査対象と同じ振る舞いをするファイアウォールシミュレータに仕立て上げる。このシミュレータ上でいろんなパケットの通過シミュレーションを行い、パケットの通過 / 不通過の状況からファイアウォールに設定したルールによって予定通りのポリシーが実現されているかを確認する。

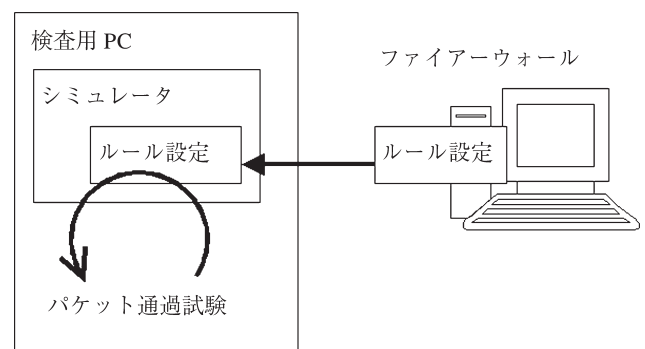


図.1 シミュレータによる検査

3.2 ブラックボックステストによる検査

実際のファイアウォールに対して様々なパケットを送り込むことにより、直接ファイアウォールの検査を行う（図.2）。

検査用のパソコンをファイアウォールの両側のネットワークに接続し、各種の検査用パケットを直接送り込む。必要なパケットが通過しているか、あるいは不必要なパケットが通過してしまっていないかを確認することにより、ファイアウォールにおいて予定通りのポリシーが実現されているかを確認する。

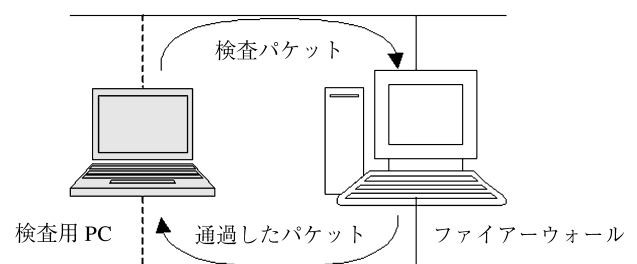


図.2 ブラックボックステストによる検査

3.3 比較検討

シミュレータにより確認する手法では、ブラックボックステストと比べてパケットの通過試験を短時間で行うことが可能であるので、より多数の通過試験を行うことができる。しかし、ルール設定の仕方はファイアーウォール製品ごとに異なるので、対象とするファイアーウォール製品ごとにルールファイルのパーサを作成する必要がある。また、対象となるファイアーウォールを正確にシミュレートするシミュレータを作成するのは困難である。

これに対して、ブラックボックステストによる手法ではファイアーウォールの種類に依存せずに検査を行うことができるので、汎用的なツールを作成することができる。ただし、ネットワーク上を実際にパケットを通過させるためすべてのパケットの通過試験を現実的な時間内に行うことは不可能であるので、一部のパケットを用いた通過試験の結果からポリシーの適合性の判断を行う必要がある。

今回はツールの汎用性を考慮し、ブラックボックステスト手法を選択した。

4. 特長

今回開発したファイアーウォール検査ツールは以下のような特長を持つ。

- (1) 1台の検査用パソコンで検査が可能
 これまでファイアーウォールの通過試験を行うには、ファイアーウォールの両側に広がる多階層のネットワーク上の2箇所にパソコンを設置して通信を行う必要があった。しかも、この方法では物理的に設置不可能な場所との検査はできなかった。
 今回のツールではネットワークインタフェースを2枚持ったパソコンを使用して、1台のパソコンのみで検査を行うことができる。
- (2) ファイアーウォールの種類に依存しない
 人手による机上でのシミュレーションや、シミュレータを用いた検査とは違い、実際のファイアーウォールに対して検査パケットを通過させて検査を行うので、ファイアーウォールでのルール設定方法やファイアーウォールの実現方法には依存しない。
- (3) 多階層ネットワーク構成に対応
 検査パケットを作成する際には、ファイアーウォールに直接接続されているネットワーク上のノードの検査だけでなく、ネットワークシミュレート機能により、ファイアーウォールの両側にある多階層のネットワーク構成の検査も行う。
- (4) ファイアーウォールルール以外のセキュリティホールの検査も可能
 通常ファイアーウォールを通過するパケットだけでな

く、通常のネットワークの運用では発生しないようなパケットを用いた検査も行うので、アドレスを偽造することにより不正侵入を試みるスプーフィングへの対策不足やルーティングミスなどのセキュリティホールも発見できる。

- (5) ネットワークの構成やファイアーウォール稼働中の負荷に応じた検査

検査パケットの数やパケット送信間隔などを自在に設定できる。したがって、サーバなど重点的な検査が必要なノードの数や検査に費やせる時間に応じて検査パケット数を調整できる。また、ファイアーウォール稼働時など検査による負荷を減らしたいときにはパケット送信間隔をあげることにより、ファイアーウォールへの負荷を減らすことができる。

5. 検査ツールの構成

ファイアーウォール検査ツールは、パケットの送受信を行ってそれぞれのパケットに対するファイアーウォールの反応を確認するパケット送受信エンジンと、どんなパケットを用いてファイアーウォールの検査を行うかを決定する検査リスト生成エンジンから構成される。

図.3に示すように、ネットワーク情報よりリスト生成エンジンを用いて検査パケットリストを生成し、この検査パケットリストに従ってパケット送受信エンジンで各パケットの検査を行い、結果を出力する。

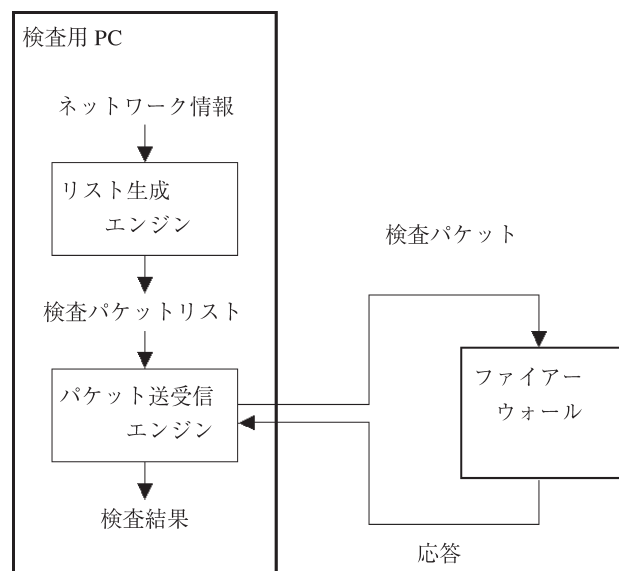


図.3 検査ツール構成

5.1 パケット送受信エンジン

パケット送受信エンジンは、与えられるIPパケット情報に従った発アドレスや宛アドレス、サービスポート番号を持つパケットをEthernetパケットレベルから生成し、そのパケットをファイアーウォールへ送信する。

送られたパケットに対して、ファイアーウォールは設定されているルールに従って以下のような反応をする。

ファイアーウォールを通過させ、宛先ノードへ送信する。

発信元ノードにエラーを意味するパケットを返す。

パケットを破棄する。

パケット送受信エンジンはファイアーウォールの両側のネットワークを監視してファイアーウォールから送り出されるパケットを検出し、各パケットに対するファイアーウォールの反応を検査結果として出力する。

5.1.1 多階層ネットワークシミュレーション

パケット送受信エンジンに与えられるパケット情報は、プロトコル（TCPかUDP）、発IPアドレス、宛IPアドレス、サービスポート番号、などである。

この時に与えるIPアドレスは、ファイアーウォールの両側にあるファイアーウォールが所属するネットワーク上に存在するノードのアドレスだけでなく、ルータを介した先にある多階層ネットワーク上に存在するノードのIPアドレスも使用する。

パケット送受信エンジンではIPパケットの発IPアドレスおよび宛IPアドレスにこれらのアドレスを使用してファイアーウォールに直接送り込むことにより、ルータ越しに送られたパケットであるように見せかける。また、ファイアーウォールからルータ越しに送られるパケットをパケット送受信エンジンで横取りすることにより、ルータ越しのパケット送信が行われたかのように見せかける（図.4）。

これによって、ファイアーウォールの実稼動時にファイアーウォールを通過し得るあらゆるパケットに対する検査を可能にしている。

5.1.2 擬似アドレス解決

ファイアーウォールがIPパケットを同一ネットワーク上のノードに送信する際には、ファイアーウォールはIPアドレスに対応するEthernet上でのネットワークアドレスの取得を行うアドレス解決を試みる。

実稼動時にはファイアーウォールからのアドレス解決要求に対して当該ノードが応答を返すことによりアドレス解決が行われ、ファイアーウォールはネットワークアドレスを取得できる。ファイアーウォールはそのネットワークアドレスを用いて当該ノードにIPパケットを送る

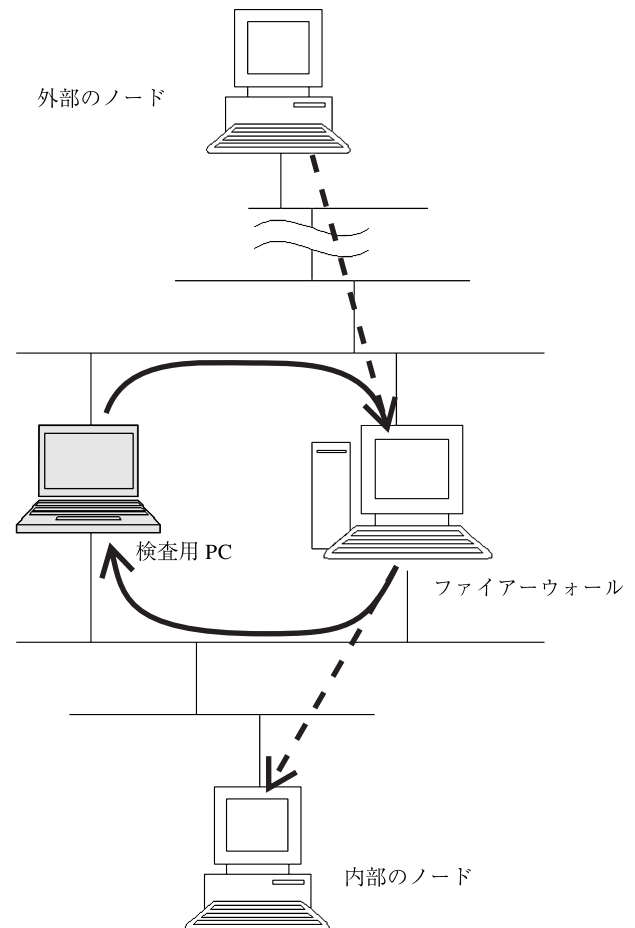


図.4 多階層ネットワークシミュレーション

ことができる。

しかし、検査時には検査パケットの宛IPアドレスのノードは存在するとは限らない。その場合にはアドレス解決応答が行われないので、検査パケットがファイアーウォールから送られなくなってしまい、検査パケットがファイアーウォールのルールを通過したのかも判らなくなってしまう。そこで、ファイアーウォールからのアドレス解決要求に対し、パケット送受信エンジンが擬似回答を返すことで擬似的にアドレス解決を行わせる。

これによって、検査パケットがファイアーウォールから送信されるようになり、ファイアーウォールでのルール通過の判定ができるようになる。

5.2 検査リスト生成エンジン

検査リスト生成エンジンは、対象となるファイアーウォールの検査を行うために必要な検査パケットのリストを生成する。

検査に使用するパケットは発アドレス、宛アドレス、サービスポート番号などを変えながらすべての組み合わせで検査することが望ましい。しかし、すべての組み合わせ

の検査を許容できる時間内に行うことは不可能であるので、一部のパケットのみを使用して検査を行うことになる。検査可能なパケット数は限られているので、アドレスやサービスポート番号をランダムに選んでは効率が悪くなる。したがって、検査パケットのアドレスやサービスは、ファイアーウォールの運用時に使用されるアドレス付近に絞り込んで検査を行う必要がある。

検査リスト生成エンジンでは、内部側のネットワークに存在するアドレスと外部側のネットワークに存在するアドレスや、それらのアドレスの中で重要なアドレスなどの分類を元に、検査パケットのリストを生成する。

5.2.1 重要度別の分類

IPアドレスは内部側のネットワークに存在するアドレスと外部側に存在するアドレスに分類することができる。また、それらのネットワーク上のノードは必ず検査しなくてはならないノードのカテゴリや、グループ中のいくつかについて検査すれば良いカテゴリなど、重要度によって分類することができる。サービスポート番号についても同様に重要度による分類ができる。そして、それぞれのカテゴリに対してそれらの中からどの程度のノードを選択するかの選択度を設定する。

例えば、ファイアーウォールで保護されたネットワーク内にあるサーバなどのノードは重要度大のカテゴリに分類し、ファイアーウォール外部からのアクセス検査を必ず行うようにする。また、クライアントのノードは重要度中のカテゴリに分類し、ランダムに選択した数箇所のノードのみを検査するなどのように設定する。

5.2.2 検査パケットの生成

ファイアーウォールの稼働時にファイアーウォールに送られてくるパケットは、外部のネットワークから来るものと内部のネットワークから来るものがある。ファイアーウォールの検査は、これらの両方向のパケットに対して行う必要がある。

外部側のネットワークから送られてくるパケットは、通常は外部ネットワーク上のノードから内部ネットワーク上のノードへあてたパケットである。これらのパケットに対する検査が、ファイアーウォールのルールの主要検査項目となる。また、発アドレスや宛アドレスが通常とは異なるパケットの通過を許可していた場合は、セキュリティホールとなるので、これらのパケットに対するファイアーウォールの振る舞いも検査する。これらのパケットは、発アドレスと宛アドレスがそれぞれ内部側と外部側のどちらのネットワークに含まれるかによって表.1のように分類することができる。

表.1 外部ネットワークから送られるパケットの分類

| | | 宛アドレス | |
|-------|----------|------------------------|--------------------|
| | | 内部ネットワーク | 外部ネットワーク |
| 発アドレス | 内部ネットワーク | Spoofting パケット 検査領域 | Routing ミス 検査領域 |
| | 外部ネットワーク | 通常パケット 検査領域 | |

通常パケット検査領域は、発アドレスが外部側のネットワーク上のアドレスで、宛アドレスが内部側のネットワーク上のアドレスであるパケットに対する検査となる。これらのパケットに対する検査に使用する検査パケットは、重要度ごとに定めたカテゴリ分けおよび選択度に従って発アドレスと宛アドレスを選択し、それらのアドレスを持つパケットを生成する。

発アドレスと宛アドレスが共に内部側のネットワーク上にあるパケットはIPアドレスを偽って内部側のネットワークへの侵入を試みるパケットと考えられる。このようなパケットをファイアーウォールで通過させると重大なセキュリティホールとなる。これらのパケットに対する検査は通常のパケットに対する検査とは別に選択度を設定し、内部側のネットワーク同士の検査パケットを生成する。

宛アドレスが外部側のネットワーク上にあるパケットは直接セキュリティホールとはならないが、これらのパケットの通過を許可することにより、他のノードに対する攻撃の踏み台となる恐れがあるので、これらのパケットの中継は禁止しておくべきだと考えられる。これらのパケットに対する検査も通常のパケットに対する検査とは別に選択度を設定し、検査パケットを生成する。

同様にして、内部側のネットワークから送られてくるパケットに対する検査についても、アドレスの分類および選択度に従って通常パケットおよびセキュリティホールに対する検査をそれぞれ行う。

6. おわりに

今回開発したファイアウォールチェッカーによって、ファイアウォールの潜在的なセキュリティホールを発見できるようになった。企業内ネットワークにおけるファイアウォールの検査だけでなく、産業用システムの出荷時や現場での調整時の検査などに活用できると考えている。

今後は Ethernet だけでなく ISDN ルータなどのダイヤルアップ環境でも使用可能にし、幅広い環境に対する検査ができるようにしていきたい。また、現在はテキストベースのツールであるので、GUIを使用したインタフェースを開発し、ユーザーフレンドリーな検査環境を提供していくのが今後の課題である。

商標

Ethernet は米国 Xerox 社の登録商標です。

著者所属

研究開発本部 三島 崇

研究開発本部 佐内 大司