firewalld を用いた研究室のファイアウォールサーバ構築について

三重大学工学部工学研究科技術部
中村　勝
nakamura@elec.mie-u.ac.jp

１．はじめに

研究室のファイアウォールサーバを Linux を用いて構築することとなった。使用した OS は CentOS7 である。CentOS7 から採用されたデフォルトのファイアウォール firewalld を使用し、今回はじめてファイアウォールサーバを構築したこともあり、トラブルや問題点、取り組みについて報告を行う。

２．ファイアウォールとは

インターネットと内部ネットワークの間のアクセスを制限する方法の一つ。一般的には、ネットワークがインターネットに接続するポイントに設置する仕組みで、両方向のすべての通信が、ファイアウォールを通過しない限りネットワークを超えられず、ローカルネットワークのセキュリティ方針で許可されている通信だけを通過させる。

３．ファイアウォールの要件

研究室のファイアウォールを構築するにあたり、以下の要件を満たす必要がある。

- サーバ機で構築する事
- OS は Linux
- OS はサポート期間が長い
- NAT を使用する
- 内部のサービスは DNS と telnet
- 内部から外部へのアクセスはサーバで許可された IP アドレスのみ接続可(メール,web 等)
- 外部へのサービスは無
- サーバ機で外部接続許可する PC の設定は簡易

PC は FUJITSU　PRIMERGY TX1310 M1 OS レスタイプ 500GB×1 PYT1311ZGC を使用した。
OS は CentOS7 を使用しデフォルトのファイアウォールサービス firewalld を使用して構築することとした。

３．１．netfilter と firewalld

Linux では、パケットフィルタリングの機能はカーネル内の netfilter と呼ばれるサブシステムで処理される。従来の CentOS は iptables と呼ばれるコマンドで様々な指示を行ってきたが様々な問題があったため、firewalld が導入された。firewalld では、パケットフィルタリングの処理とアドレス変換の処理を簡単にするために、ネットワークインターフェースをゾーンというグループに分けて管理する。CentOS の firewalld では、あらかじめ表 1 のゾーンが定義されている。

ゾーンは新規に作成することができるが、あらかじめ定義されているゾーンに外部インタフェース用や内部インタフェース用が用意されていることもあり、今回はデフォルトのゾーンを使用することとした。

許可 IP アドレスの追加・削除の際はコマンドラインからでも変更可能であるが、/etc/firewalld/zones/ 内のファイルを修正することでも変更可能である。

表１　あらかじめ定義されているゾーン

分類	ゾーン名	役割	デフォルト通信許可サービス
一般	public	デフォルトのゾーン。サーバなど公共の領域での利用を想定している。	dhcpv6-client,ssh
	work	業務でのクライアントコンピュータとしての利用を想定している。ほとんどのコンピュータが信頼できる環境での利用に向いている。	dhcpv6-client,ssh
	home	家庭でのクライアントコンピュータとしての利用を想定している。ほとんどのコンピュータが信頼できる環境での利用に向いている。	dhcpv6-client,mdns, samba-client,ssh
ファイアウォール	internal	ファイアウォールの内部ネットワーク側での利用を想定している。	dhcpv6-client,mdns, samba-client,ssh
	external	ファイアウォール外部ネットワーク側での利用を想定している。他のコンピュータが信頼できない環境を想定している。	ssh
	dmz	ファイアウォールの DMZ での利用を想定している。	ssh
特殊	block	受信パケットはすべて拒否	無
	drop	受信パケットはすべて破棄	無
	trusted	受信パケットの制限は行わず、すべてのネットワークコネクションを許可する。	全て

３．２．運用時のトラブル

インターフェィスの設定および上記のゾーンファイルにアクセス可能な IP の記述を行い、内部ネットワーク同士の ssh 接続の動作確認を行ったところ問題は見つからなかった。サーバにおいても DNS の動作確認のため、正引きできるかどうか確認をした。しかし、運用を開始すると ssh では FQDN にて問題なく接続出来たが telnet では FQDN では接続不可であった。そのため telnet 接続を行う PC には host.conf に接続するサーバの FQDN と IP アドレスを記述することで対応した。

firewalld には「ダイレクトルール」が使用できるため、次の試みとしてダイレクトルールを使用することとした。ダイレクトルールとは複雑なルールを設定する場合に使用される。ダイレクトルールでは「INPUT」、「OUTPUT」、「FORWARD」、「PREROUTING」、「POSTROUTING」のチェインがありこれらを使用することでパケットのフィルタリングが出来る。これらを使用して IP アドレスによる許可設定をすることとした。しかし、設定を行っても firewalld が動作しない状況がある事に気づく。コンソールより一度 firewalld を起動すると動作を行うが、PC 起動時は動作しない。Linux で IP フォワードを有効にするには、「net.ipv4.ip_forward=1」が必要（デフォルトでは net.ipv4.ip_forward=0）との情報を得た。CentOS7 では該当ファイルが「/etc/sysctl.d/ipv4.conf」であるのでここに記述した。

表 2　チェインとテーブル

チェイン名	役割	利用できるテーブル
INPUT	受信するパケットとして適切かをチェック	nat,mangle
OUTPUT	送信するパケットとして適切かをチェック	filetr,mangle
FORWARD	転送するパケットとして適切かをチェック	filetr
PREROUTING	受信したパケットを変換する	filetr, nat,mangle
POSTROUTING	送信したパケットを変換する	nat

４．おわりに

今回、はじめてファイアウォールサーバを構築したこともあり試行錯誤の末、使用できるレベルまで構築することが出来たが、使用状況を把握し問題点があれば改善する必要がある。今回の情報収集はインターネットのみで行ったが、インターネット上ではほぼ掲載されていない設定が CentOS7 関連の書籍に記述してあり、改めて書籍の重要性を知ることとなった。

参考文献

1) 久米原 栄(2000)　Linux ネットワーク ファイアウォール管理者ガイド　ソフトバンクパブリッシング

2) デージーネット(2015)　『CentOS7 システム管理ガイド systemd/NetworkManager/Firewalld 徹底攻略』　秀和システム