目次

Firewall の設定 (FirewallD)

Ubuntu Linux 標準の Firewall Framework である ufw ですと、簡易的なフィルタ程度であればコマンドラインで設定できるのですが、
NAPT などが必要となると iptables の設定を直接ファイルに記述する必要があり、ちょっと力不足な印象です。

そこで Firewall を統合的に管理できる、FirewallD を v2.2.0 から採用しています。

説明

Fedora Project Wiki "FirewallD" のページ がリファレンスです。
内部の実装についての概要を知るには、 Linux女子部 firewalld徹底入門 - slideshare がオススメです。

設定

MA-E3xx での初期設定は、下記のとおりです。

Zone	interfaces	sources	services	ports	masquerade	forward-ports	icmp-blocks	rich rules	notes
drop					no				全ての内向きパケットは破棄 (Drop) (変更不可)
block					no				全ての内向きパケットは拒絶 (Reject) (変更不可)
public			dhcpv6-client, ssh		no				選択された内向きのコネクションのみ Accept (公共エリア用)
external	ppp0		ssh		yes				選択された内向きのコネクションのみ Accept (IP Masquerade が有効な外部ネットワーク)

Zone	interfaces	sources	services	ports	masquerade	forward-ports	icmp-blocks	rich rules	notes
dmz[1)]			ssh		no				選択された内向きのコネクションのみ Accept (非武装地帯のコンピュータ用)
work			dhcpv6-client, ipp-client, ssh		no				選択された内向きのコネクションのみ Accept (業務エリア用)
home			dhcpv6-client, ipp-client, mdns, samba-client, ssh		no				選択された内向きのコネクションのみ Accept (自宅エリア用)
internal			dhcpv6-client, ipp-client, mdns, samba-client, ssh		no				選択された内向きのコネクションのみ Accept (内部ネットワーク用)
closed[2)]	ppp100, ppp50x				yes				全ての内向きパケットを受入 (Accept) (閉域網用)
trusted	eth0, eth1, br0, lo				no				全ての内向きパケットを受入 (Accept)

※ 注

FirewallD の標準設定では、default zone は “public” となっていますが、“dhcpv6-client” が有効になっているのが好ましくないので
MA-E3xx では “dmz” (SSH のみ有効) にしています。
default zone を “drop” にしてしまうと、Network Interface (USB Ethernet, PPP など) を追加した場合、明示的に zone に追加しない限り
PREROUTING で叩き落とされて 一切通信ができなくなる ためお勧めできません。

設定サンプル

ポート転送 (DNAT)

ポート転送 (DNAT, 送信元アドレス制限)

1)
default zone
2)
MA-E3xx で追加した zone です