iptablesでDNSクエリーを引っ掛けてみた

其田 学

iptableとDNSといえば？

u32 module

- パケットに対して、色々なマッチングパターンを書けるモジュール。
- 標準ライブラリなので、追加でインストールする必要はない。

例：qname=isc.org. qtype=ANY

```
iptables –m u32 –u32 \
0>>22&0x3C@20&0xFFDFDFDF=0x03495343&&
0>>22&0x3C@24&0xFFDFDFDF=0x034f5247&&
0>>22&0x3C@28&0xFFFFFF00=0x0000FF00%
```

U32モジュールの欠点

- ルールを作るのが難しい
  - ツールありますけどね。
  - generate-netfilter-u32-dns-ruleとかで検索
- 静的なマッチングしかできない。
  - QNAMEは可変長なので、決め打ちしたQNAMEしかマッチングできない。
  - QNAMEの後にQTYPEが来るので、QTYPEだけのマッチングもできない。

作りました

- iptables-ext-dns(xt_dns)
  - https://github.com/mimuret/iptables-ext-dns

xt_dns module

- 主な機能
  - DNS Headerのflag bit系でのマッチング
  - QNAMEでのマッチング（後方一致有り）
  - QTYPEでマッチングが可能
  - IPv4/IPv6, TCP/UDPに対応
- 動作環境
  - Kernel 2.6以降

使用例

- example.jpをマッチングする場合

```
iptables -A INPUT  -m dns --qname example.jp
ip6tables -A INPUT  -m dns --qname example.jp
```

使用例

- $(randam).example.jpをマッチングする場合

```
iptables -A INPUT  -m dns –rmatch --qname example.jp
ip6tables -A INPUT  -m dns –rmatch --qname example.jp
```

使用例

- QTYPEがANYのものをマッチング

```
iptables -A INPUT  -m dns –qtype ANY
ip6tables -A INPUT  -m dns --qtype ANY
```

使用例

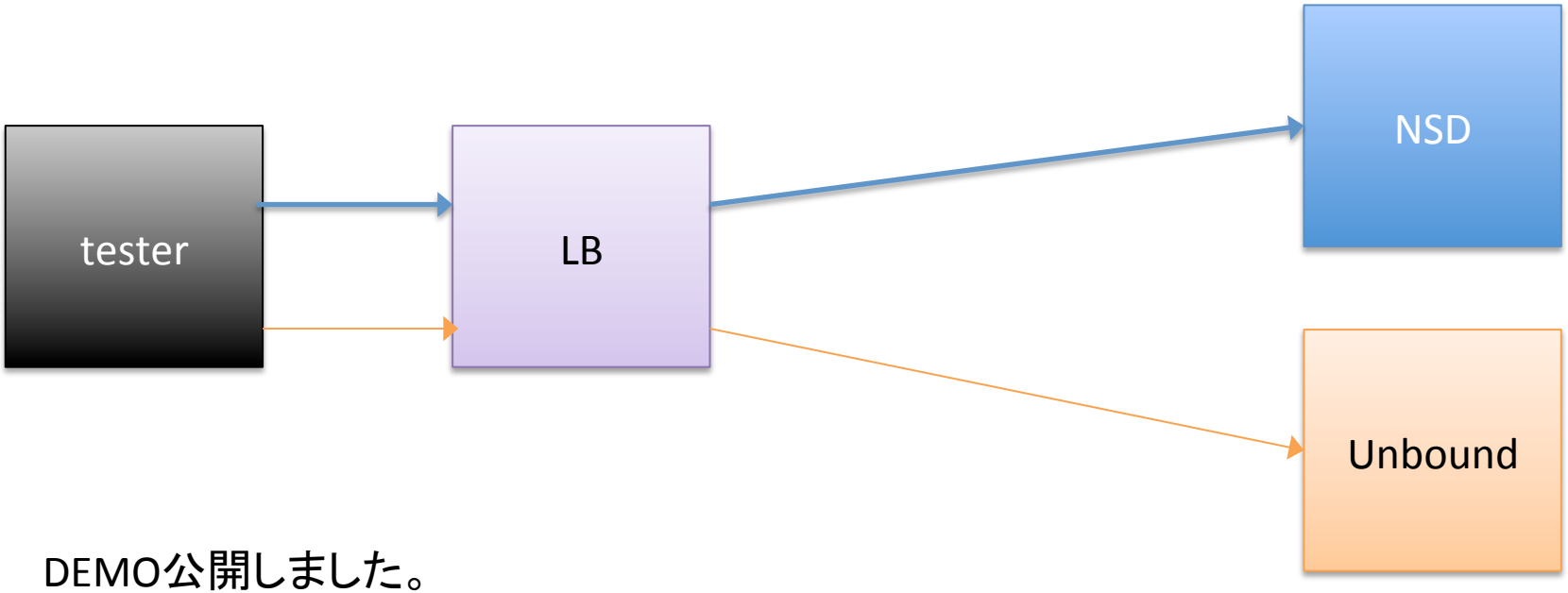
- マッチングしたものは、iptablesのターゲットモジュールで処理できます。
  - DROP,REJECT
  - LIMIT
  - MARK
  - LOG
  - などなど
- 使い方いろいろ

想定している使用例

- DDoSに使用されているドメイン名をMARKしてLVSを使って通常とは別のサーバへフォワード
- ランダムサブドメイン攻撃を受けた時に、攻撃を受けているドメイン名とゾーンの中にある最大のドメイン名のサイズ以上でマッチングしてDROP

ちょっと構築してみた

- LBの下にNSDとUnboundを置く
- LBのiptablesでRD bitを見てMARKをつける。
- IpvsでNSDとUnboundを振り分ける。



DEMO公開しました。
https://github.com/mimuret/iptables-ext-dns-demo

今後の開発予定

- dnsset（開発中）
  - ipsetのqname版
  - xt_dnsは実はたくさんルール書くとQPSがガタ落ちします。
  - dnssetは複数のQNAMEを木構造のデータベースに入れて、複数のマッチングをいっぺんにやってしまうコンセプトです。

今後の開発予定(ネタ編）

- DNS（妄想中）
  - パケットの処理を行うモジュール
  - NOERRORとかREFUSEDとかDNS的に正しいresponseを返したいなーと思ってます。
- DNSTAP（ネタ）
  - 行ってみただけ

今後の開発予定

- ご意見は下記のissueにお願いします。
  https://github.com/mimuret/iptables-ext-dns
- Pull reqもお待ちしてます。。。
- おしまい。