自宅サーバを nftables で守ってみる

東京エリア・関西合同 Debian 勉強会

Norimitsu SUGIMOTO (杉本 典充)
dictoss@live.jp

2023-11-18

アジェンダ

- 自己紹介
- nftables とは
- nftables の自分的運用ルールと悩み
- nftables の運用ルール変更方針と改修
- まとめ
- 参考資料

自己紹介

- Norimitsu SUGIMOTO (杉本 典充)
- dictoss@live.jp
- Twitter: @dictoss
- Debian を使い始めたのは 3.1 sarge が testing の頃
- 仕事はソフトウェア開発者をやってます
- python と Django の組み合わせで使うことが多いです

nftables とは

nftables とは

- Linux のネットワークフィルタリング機能を操作するフロントエンドコマンド
- iptables の後継
- web サイト：https://www.netfilter.org/
- 「ntf サブコマンド」 のような感じで使う
  - 例：nft list ruleset
- 2019 年 12 月 東京エリア Debian 勉強会で使い方を発表「Debian 10 buster で nftables を使ってみる」[1]
- 今回は nftables を運用している中での困りごととその改善のお話

[1] https://tokyodebian-team.pages.debian.net/pdf2019/debianmeetingresume201912.pdf

nftables の自分的運用ルールと悩み

nftables の自分的運用ルールと悩み

- 少し前までは以下のような感じで運用
  - fail2ban など動的なルールのソフトは使わない
  - http
    - インターネット公開するブログサーバのため制限なしで許可
  - ssh
    - プライベート IP アドレスは 22/tcp で許可
    - 外部からアクセスできる ssh はポート番号を変更した上で制限なしで許可
    - sshd は ssh 鍵認証のみ許可 (パスワード認証は無効)

nftables の自分的運用ルールと悩み

以前、運用していた nftables 設定

```
# cat /etc/nftables.conf
table ip filter {
    chain input {
        type filter hook input priority filter; policy drop;
        ct state established,related accept
        ct state invalid drop
        iif "lo" accept
        icmp type { echo-request, echo-reply } accept
        tcp dport ssh ip saddr { 10.0.0.0/8, 172.16.0.0/12,
          192.168.0.0/16 } accept
        tcp dport 40022 ip saddr { 0.0.0.0-255.255.255.255 } accept
        tcp dport http ip saddr { 0.0.0.0-255.255.255.255 } accept
    }
    chain forward {
        type filter hook forward priority filter; policy accept;
    }
    chain output {
        type filter hook output priority filter; policy accept;
    }
}
```

nftables の自分的運用ルールと悩み

- 悩み
  - やはり ssh のポート番号を変えているくらいでは手当たり次第に攻撃される
  - ssh ログインは ssh 鍵認証のみ許可するよう設定変更しているとはいえ、なんか怖い
  - サーバを乗っ取られるのはまずい
  - ssh のポート番号を防御する対策を何かしたい
- 前提
  - サーバは固定グローバル IP アドレス、または DDNS
  - アクセス元の自宅の固定回線は固定グローバル IP アドレス環境ではない
  - アクセス元のモバイル回線は固定グローバル IP アドレス環境ではない

nftables の運用ルール変更方針と改修

nftables の運用ルール変更方針

- (ポート番号を変えて) 外部からアクセスできる ssh は基本的に drop するルールに変更
- 個別に許可する ssh 通信元のネットワーク
  - 自宅の固定回線は動的なグローバル IP アドレスだが ISP で範囲は決まっている
  - 自分のモバイル回線の出口のグローバル IP アドレスはキャリアで範囲は決まっている
  - → 調べて個別に開ければよいのでは？
- あきらめること
  - お店などの公衆 Wi-Fi からのアクセス

情報収集：アクセス元のIPアドレス情報

- 光回線
  - OCN
    - 公開していない模様
    - 実際に割り当てられるグローバル IP アドレスを JPNIC WHOIS Gateway[2] で検索して範囲を調べる
- モバイル回線
  - ドコモ (sp モード) `https://www.docomo.ne.jp/service/developer/smart_phone/spmode/`
  - KDDI (povo) `https://www.au.com/developer/android/kaihatsu/network/`
  - IIJmio
    - 公開していない模様
    - 実際に割り当てられるグローバル IP アドレスを JPNIC WHOIS Gateway で検索して範囲を調べる

[2] `https://www.nic.ad.jp/ja/whois/ja-gateway.html`

nftables 設定ファイル改修方法

- nftables の設定ファイルの書き方
  - Scripting
    `https://wiki.nftables.org/wiki-nftables/index.php/Scripting`
- 便利な構文
  - define
  - set
  - include

作成した nftables 設定 (フィルタルール)

```
# cat /etc/nftables.conf
#!/usr/sbin/nft -f
define range_ipv4_private = { 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 }

table ip filter {
  set allowed_iplist_sshd {
    type ipv4_addr
    flags interval
    auto-merge
    comment "allowd iplist to sshd"
  }
  chain input {
    type filter hook input priority filter; policy drop;
    ct state established,related accept
    ct state invalid drop
    iif "lo" accept
    icmp type { echo-request, echo-reply } accept
    tcp dport 22 ip saddr { $range_ipv4_private } accept
    tcp dport 40022 ip saddr @allowed_iplist_sshd accept
    tcp dport http ip saddr { 0.0.0.0-255.255.255.255 } accept
  }
  chain forward {
    type filter hook forward priority filter; policy accept; }
  chain output {
    type filter hook output priority filter; policy accept; }
}
include "/etc/nftables.d/*.nft"
```

フィルタルール 解説

- define 変数
  - フィルタルールで define を指定する場合は # をつける
- set セクション
  - type
    - ipv4_addr は IPv4 の集合という指定
    - そのほかは ipv6_addr、ether_addr、inet_proto、inet_service、mark など
  - flags interval、auto-merge
    - IP アドレスを範囲指定可能とするフラグ
    - auto-merge は複数の IP アドレスの範囲が重複していた場合に自動で範囲調整するフラグ
- @allowed_iplist_sshd (set 変数)
  - フィルタルールで set を指定する場合は @ をつける

作成した nftables 設定 (set アドレス追加)

```
# cat /etc/nftables.d/nftables_set_jp-docomo.nft

#!/usr/sbin/nft -
define element_ip4_jp_docomo_servers = {
  1.66.0.0/16,
  1.72.0.0/16,
  1.73.0.0/16,
  1.75.0.0/16,
  1.78.0.0/16,
  1.79.0.0/16,
  (省略)
  49.109.0.0/16,
  160.249.0.0/16,
}

add element ip filter allowed_iplist_sshd {
  $element_ip4_jp_docomo_servers }
```

あとは systemctl restart nftables で適用すれば OK ルールの出力は nft list ruleset を実行

まとめ

まとめ

- nftables のフィルタリングルールを効率的に書く方法を紹介しました
- define、set、include を使いこなすと便利
- 今回は「基本 drop、個別 accept」のパターンを紹介しましたが、逆の「基本 accept、個別 drop」も同じように書ける
- インターネットは便利ですが、攻撃もあり防御対策も必要
- github で nftables の設定を公開中 [3]

[3] https://github.com/dictoss/utils/tree/master/conf/nftables/sample_jp-mobile

参考文献

- nftables wiki - Scripting
  https://wiki.nftables.org/wiki-nftables/index.php/Scripting
- Linux における新たなパケットフィルタリングツール「nftables」入門
  https://knowledge.sakura.ad.jp/22636/