Engineer

ファイアウォール

どの通信を通すかを決める規則の集合

どのようなものか

ファイアウォールは、ネットワーク経路で、各パケットや接続を規則の一覧と比べ、通すか、捨てるか、拒否を返すかを決めるフィルターです。保護するマシン上のソフトウェア、二つのネットワーク間の専用機器、クラウド事業者が仮想マシンの前で動かすサービス、といった形があります。Linuxの管理者は、同じものをパケットフィルターとも呼び、クラウド事業者は、セキュリティグループなどの名前で提供します。複数ある場合は、事業者側とホスト側というように、層になることが多くあります。

NISTの2009年9月の指針、SP 800-41 Rev. 1は、トラフィックをどこまで読むかで分類します。パケットフィルターは、パケットを一つずつ読み、アドレス、プロトコル、ポート番号を見ます。ステートフルなものは、接続も記憶します。そのため、サーバー自身が送ったリクエストへの応答を、専用の規則なしで受け取れます。アプリケーションプロキシーのゲートウェイは、接続を終端し、中のプロトコルを読みます。ホスト型は、保護するサーバーやノートPC上で動き、どのプログラムがソケットを持つかを知ります。

Linuxサーバーでは、カーネルのnetfilterの仕組みでフィルターを実行します。カーネル3.13から使えるnftablesが、古いiptablesの道具を置き換えます。ufwなどのフロントエンドは、チェーンより意図を記述したい人のために、規則を書きます。何が書いても、モデルは同じです。順序付きの一覧を上から読み、最初に一致する規則が決めます。

隣接する道具との混同もあります。ウェブアプリケーションファイアウォールは、HTTPリクエストを読み、その中の攻撃パターンを止めます。ネットワークのファイアウォールは、そこまで深く見ません。不正なアクセス元を遮断する道具は、ログを読み、問題のあるアドレスへの一時的な規則を加えるため、下の

ファイアウォールに依存します。VPNは、そもそも誰がネットワークへ入れるかを決めます。それぞれ違う問いに答え、どれも、基本の規則の一覧を置き換えません。

概念を判断に生かす

「ファイアウォールとは？」を実際の判断に生かしましょう。その概念を、開発または購入するシステムに結び付けて考えるお手伝いをします。 アカウント、パスワード、権限を整理し、業務に必要なアクセスだけを付与し、退職者の権限は当日に解除します。

サービスを見る お問い合わせ →

用語の背後にある前提を検証する

解説とリンク先の実績を参考に、プロジェクトについての質問を整理してください。ツールを選ぶ前に、前提を一緒に検討できます。 Linuxサーバーを守る1,000件のRBACルールを作成 — 1,000 セキュリティ上の穴を塞ぐアクセスルール

Linuxサーバーを守る1,000件のRBACルールを作成 お問い合わせ →

なぜ重要なのか

公開アドレスで待ち受けるサービスは、どれも扉です。ファイアウォールは、存在する扉の一覧です。実際にチームが決めるのは、置く場所、既定で許すもの、変更できる人の、三点です。

事業者側のものは、マシンへ届く前に止め、ホストのroot権限を奪われても動き続け、サーバーのCPUを使いません。規則は、サーバー自身の設定の外、管理画面やAPIにあるため、コードにしなければ、ずれていきます。ホスト側のものは、マシンとともに移り、一つのポートの通信頻度を制限でき、マシン自身から試せます。ただし、侵害されたrootアカウントや、自分で規則を管理するソフトウェアは、書き換えられます。両方を使うのは、一般的で妥当ですが、二つの一覧を合わせる負担があります。ポートを一つ開閉するたびに、二か所を変えます。

二点目は、既定の方針です。NISTは、明示して許可したもの以外を、すべて拒否するよう勧めます。受信では、ほぼ合意されています。送信の制限には、利害の衝突があります。侵害されたサービスの到達先を絞れますが、宛先ごとの規則を加えるまで、パッケージ更新、証明書更新、監視も動かなくなります。

三点目は、管理の責任です。既定で拒否するものの正しさは、誰かが宣言したポート一覧にかかっています。役立つ成果物は、バージョン管理し、稼働中の規則と照合する、その一覧です。主要なLinuxディストリビューションでは、ソフトウェアは無料です。費用がかかるのは、宣言を正しく保つために、目を配る作業です。ファイアウォールは、二番目の防御線でもあります。ループバックへバインドしたサービスは、規則にかかわらず外から届きません。どこからでも待ち受けるサービスの前に拒否規則を置くより、強い保証です。

実際の活用例

あるホストでは、SSHポートへの接続頻度の制限が、一年間、規則一覧にありながら、一パケットも受け取りませんでした。上の、より広い許可規則が、先に一致したためです。状態を示す道具は、一年中、制限を載せました。実際に存在したので、表示は正しかったのです。検査を、存在ではなく位置を読むものへ書き換えました。番号付き規則と、カーネルが実際に使うチェーンの順序を、意図したものと比べます。各ポートに規則を一つ置き、必ずプロトコルを指定します。SSHは接続頻度を制限し、別の許可は置きません。五つの公開ポートをまとめて宣言し、集合として確かめます。宣言にない開いたポートがあれば失敗し、セキュリティレポートは、パケットが出会う順序で一覧を示し、読み方も付けます。

最初のサーバーは、手で作り、後からファイアウォールを加えたため、新しいマシンへ、インターネットから届く時間がありました。別の事業者の二台目では、マシンより先に、専用のplayでファイアウォールを作ります。新しいマシンが、最初から規則を持ってインターネットへ接続します。事業者は、タグで結び付けるため、先にタグを作ります。対象とするタグが、存在する必要があるためです。各事業者のものを、通常のHTTPタスクで、そのREST APIへ直接書きます。タスクはドライランで何もしません。そのため、ファイアウォール用のplay自体で変更を予行します。事業者のファイアウォールは、作成が無料で、また削除できるためです。

コンテナーは、ファイアウォールに触れず、通り抜ける場合があります。Dockerは、カーネルのパケットフィルターへ自分の項目を書きます。公開したコンテナーポートは、ホストを強化するロールの規則より先に一致するため、指示した方針にかかわらず、外から届くことがあります。このプラットフォームは、PodmanとQuadletを通じ、systemdでコンテナーを動かします。ホストのネットワークを共有し、ポートを公開しないため、規則を迂回させる対象のコンテナーポートがありません。

問題が起きるところ

一覧にある規則が、一度も動きません。 上から評価し、最初の一致を使うため、広い許可を、狭い制限や拒否より上へ置くと、その制限や拒否は一切働きません。一覧には、両方が残ります。カーネルと同じように、番号を付けて順に読み、具体的なものを一般的なものより上へ置き、外のマシンから試します。

```
ufw status numbered
nft list ruleset
```

拒否したポートで、コンテナーが応答します。 Dockerは、カーネルのNATテーブルでトラフィックを転送して、ポートを公開します。この転送は、ufwがフィルターするチェーンへ届く前に起こります。Docker自身の文書も、実質的にファイアウォールの設定を無視すると述べます。ループバックだけへ公開するか、事業者側のものを前に置くか、前述のように、ポートを公開せず動かします。

IPv4を厳しく制限しても、IPv6が開いています。 iptablesは、二つのアドレスファミリーに別々の規則を持ち、ufwは、既定値のファイルでIPv6を有効にした場合だけ、IPv6の規則を書きます。公開IPv6アドレスを持ち、IPv4用しかないホストは、待ち受ける全ポートが露出します。両方を見る、`inet` ファミリーのnftablesのテーブルを使うか、両方の一覧を監査し、外からIPv6アドレスをスキャンします。

有効にした瞬間、SSHが固まります。 SSHの規則より先に既定の拒否を有効にしたか、デーモンのポートを変えても、規則が22のままです。先にSSHの規則を加え、別のウィンドウに事業者のコンソールを開き、数分後の自動ロールバックを予約します。新しいセッションで接続できたら、予約を取り消します。

書いた人の意図より広く、規則が開きます。 ufwでプロトコルなしにポートを指定すると、TCPとUDPの両方に開きます。全規則へプロトコルを指定し、想定する公開範囲をまとめて宣言します。余分なものが、監査まで待たず、検査を失敗させるためです。

参考資料

- ファイアウォール — 各出典へのリンクを添えた、NIST文書の定義です。
- SP 800-41 Rev. 1：ファイアウォールとその方針の指針 — NISTによる、種類、既定の拒否方針、規則の管理です。
- ufw(8) — 規則の順序と `limit` 規則を含む、Ubuntuのフロントエンドです。
- nftablesのWiki — iptablesを置き換える仕組みについての、netfilterプロジェクトの文書です。
- パケットフィルターとファイアウォール — 公開ポートが、ホストの規則を迂回する仕組みについての、Docker自身の説明です。



用語集

実際の制約に合わせて選ぶ

デプロイの流れ、運用上のリスク、緊急対応の担当者をお知らせください。検査、復旧手段、明確な責任の所在を伴う変更の範囲を定められます。

料金を見る お問い合わせ →

用語を実務に結び付ける

「ファイアウォールとは？」がお客様の組織にどう当てはまるかをご相談ください。現在のシステムの具体例が一つあれば、話を始められます。

サービスを見る

welcome@engineer.company +45 50 10 61 84 デンマーク、コペンハーゲン

このページを持ち歩く

連絡先カード

心を込めて丁寧に制作： D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

著作権 © 2025 – 現在 · Engineer ApS · すべての権利を留保します。

印刷元： https://engineer.company/ja/glossary/firewall/