perplexity

Je veux intégrer cela dans mon grand projet de développement.

Recommencer en décrivant où cela devrait se trouver dans l'arboresence.

Pour intégrer la gestion du firewall **OPNsense** dans ton grand projet de développement, il est recommandé de placer toute la configuration et l'automatisation associées dans un module dédié à l'infrastructure réseau, à l'intérieur de l'arborescence du projet. Cela garantit une séparation claire des responsabilités, une gestion versionnée de la sécurité réseau, et la possibilité d'automatiser le déploiement et la maintenance via Infrastructure as Code (IaC).

Où placer OPNsense dans l'arborescence de ton projet

Voici un exemple d'arborescence enrichie :

```
starterkit-parent/
├── ...
├── infrastructure/
│   ├── network/
│   │   ├── opnsense/
│   │   │   ├── terraform/                    # Scripts Terraform/OpenTofu pour OPNsens
│   │   │   │   ├── main.tf
│   │   │   │   ├── variables.tf
│   │   │   │   ├── firewall_rules.tf
│   │   │   │   ├── interfaces.tf
│   │   │   │   ├── aliases.tf
│   │   │   │   ├── outputs.tf
│   │   │   │   └── provider.tf
│   │   │   ├── scripts/                      # Scripts Python/Bash pour backup, monito
│   │   │   │   ├── backup_config.py
│   │   │   │   ├── restore_config.py
│   │   │   │   ├── validate_rules.py
│   │   │   │   └── ...
│   │   │   ├── docs/
│   │   │   │   ├── best_practices.md         # Documentation des règles, segmentation,
│   │   │   │   ├── network_architecture.md
│   │   │   │   └── ...
│   │   │   └── env/                          # Fichiers de variables par environnement
│   │   │       ├── dev.tfvars
│   │   │       ├── test.tfvars
│   │   │       └── prod.tfvars
│   │   └── ...
│   └── ...
├── ...
```

Démarche à suivre pour préparer ce travail

1. **Définir l'architecture réseau cible**
   - Documente les segments, VLANs, zones (LAN, DMZ, IoT, etc.), points d'accès, et le schéma d'adressage IP[1] [2] [3].
   - Précise les flux autorisés/interdits entre zones, en appliquant le principe de moindre privilège et la segmentation stricte[1] [4] [3].
2. **Rédiger la politique de sécurité et les bonnes pratiques**
   - Prévois une politique restrictive par défaut (tout bloquer, n'autoriser que ce qui est nécessaire)[1] [4].
   - Applique les recommandations de hardening : mises à jour régulières, accès admin limités, 2FA, désactivation des services inutiles, sauvegardes régulières, surveillance des logs, etc.[4].
3. **Préparer les fichiers Terraform/OpenTofu**
   - Utilise un provider Terraform compatible OPNsense (ex : browningluke/opnsense).
   - Organise les fichiers :
     - `interfaces.tf` pour les interfaces réseau,
     - `aliases.tf` pour les groupes d'IP/ports,
     - `firewall_rules.tf` pour les règles par zone,
     - `variables.tf` pour les paramètres (IPs, ports, VLAN),
     - `provider.tf` pour la connexion à l'API OPNsense,
     - `outputs.tf` pour les informations utiles (adresses, statuts).
   - Prévois des fichiers `.tfvars` pour chaque environnement (dev, test, prod, etc.).
4. **Automatiser et documenter**
   - Ajoute des scripts Python/Bash pour :
     - Sauvegarder/restaurer la configuration OPNsense,
     - Valider la conformité des règles,
     - Tester les flux réseau,
     - Gérer les mises à jour et les alertes.
   - Rédige une documentation claire : schéma réseau, justification des règles, procédures de déploiement et de restauration, gestion des incidents.
5. **Intégration dans la chaîne CI/CD**
   - Ajoute des jobs CI pour valider et appliquer la configuration réseau lors des déploiements d'environnements.
6. **Prévoir l'évolutivité**
   - Structure le dossier pour pouvoir ajouter d'autres appliances réseau, VPN, ou équipements de sécurité à l'avenir.

Bonnes pratiques à intégrer

- **Segmentation stricte** (VLAN, zones fonctionnelles)[1] [2] [3].
- **Règles explicites et documentées** (deny all, allow explicit)[1] [4].
- **Logs et alertes sur les accès refusés/anormaux**[4].
- **Gestion des accès admin sécurisée** (IP de confiance, 2FA, désactivation SSH/root, etc.)[4].
- **Sauvegardes et restauration automatisées**[4].
- **Documentation versionnée** avec le code.

En résumé :
Place toute la gestion OPNsense dans `infrastructure/network/opnsense/` avec des sous-dossiers pour :

- IaC (Terraform/OpenTofu),
- scripts d'automatisation,
- documentation,
- fichiers d'environnement,
- et intégration CI/CD.
  Cette organisation assure une gestion professionnelle, sécurisée, et automatisée du firewall au sein de ton projet global.

⁂

1. https://helgeklein.com/blog/simple-opnsense-firewall-rules-for-a-secure-smart-home/
2. https://github.com/freedomofpress/securedrop-docs/blob/main/docs/admin/installation/firewall_opnsense.rst
3. https://docs.opnsense.org/manual/how-tos/security-zones.html
4. https://www.zenarmor.com/docs/network-security-tutorials/opnsense-security-and-hardening-best-practice-guide