Okay, compris ! On va maximiser les visuels et les tableaux pour une concision extrême.

Feuille de Notes Ultra-Visuelle - Sécurité Réseau: Pare-feu

1. Pare-feu (PF) - Principes

- **Rôle:** Barrière Inter-Réseaux. **Politique: Interdiction par Défaut.**
- **Fonctions Clés:** | Fonction | Description | |----------|----------| | **Filtrage** | Bloque/Autorise trafic (IP, Port, Proto, Flag) | | **NAT** | Modifie adresses IP/Ports (voir section 2) | | *Logs* | Enregistre événements | | *Authent.* | Vérifie identité utilisateurs (parfois) |

2. Types de PF & NAT

- **Stateful (Mémoire) > Stateless (Sans Mémoire - À ÉVITER!)**
    - **Stateful :** Suit état connexions (SYN -> SYN-ACK -> ACK). Bloque paquets hors-séquence.
        - *Règle clé :* `ALLOW ESTABLISHED, RELATED`
- **NAT (Network Address Translation) :**

Type NAT	Schéma / Description	Usage Principal	Commande `iptables` (Exemple)
Dynamique (Sortant / SNAT/Masquerade)	PC_Interne (IP_Priv:Port_Priv) → PF (IP_Pub_PF:Port_Nouveau) → Serveur_Ext	Économie IPs, Masquer réseau interne	`-t nat -A POSTROUTING -o eth0 -j MASQUERADE`
Statique (Entrant / DNAT/Port Fwd)	Client_Ext → PF (IP_Pub_PF:Port_Pub) → Serveur_Interne (IP_Priv_Srv:Port_Srv_Interne)	Rendre services internes accessibles de l'ext	`-t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 192.168.1.10:8080`

3. Filtrage - Règles & Ordre

- **Critères:** `IP_Src/Dst`, `Port_Src/Dst`, `Proto (TCP/UDP/ICMP)`, `Flag_TCP (SYN/ACK/FIN/RST)`, `Interface (eth0/eth1)`
- **Actions:** `ACCEPT`, `DROP` (silencieux, pref. ext.), `REJECT` (erreur, ok int.)
- **ORDRE CRUCIAL:** 1ère règle qui matche appliquée. Spécifique AVANT général. * *Exemple (Mauvais ordre -> tout passe par proxy):*
    1. `Internal -> Proxy:3128 -> ACCEPT`
    2. `Internal -> ANY -> DROP`
    3. `ANY -> DMZ_Web:80 -> ACCEPT` *(Règle 3 jamais atteinte pour Internal)*

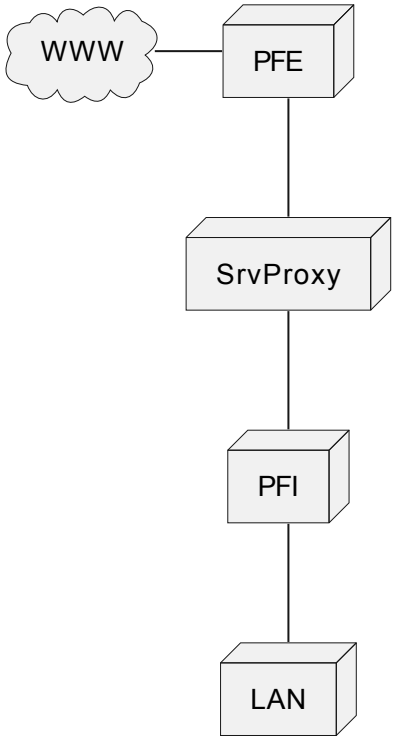
```
  *   *Bon ordre (pour exemple ci-dessus, si voulu):* Inverser 1 et 3 ou
revoir archi.
```

4. Architectures Pare-feu

Architecture	Schéma Simplifié	Sécurité	Point Clé
Simple (À ÉVITER)	`WWW --PF-- [LAN + Serveurs]`	--	Serveurs trop exposés

DMZ (1 PF)	`WWW --PF-- DMZ (Srvs)`
	`|`
	`'-- LAN`
		-	Tout repose sur 1 PF. Risque contournement.

DMZ Sandwich (2 PF - MINIMUM)	`WWW --PFE-- DMZ (Srvs/Proxys) --PFI-- LAN`	++	Isolation forte. LAN forcé via proxys.



5. PF Applicatif (WAF)

Politique WAF	Principe	Avantages	Inconvénients
Liste Blanche	Autorise SEUL le trafic connu & sûr.	Très Sûr	Maintenance, Risque Faux Positifs
Liste Noire	Bloque SEUL le trafic connu & mauvais.	Facile	Vulnérable aux 0-days
Hybride	Combinaison. CRS OWASP (ModSecurity)	Bon compromis	Configuration peut être complexe

- *Ex règle (ModSecurity) :*
  `SecRule ARGS "<script>" "deny,status:403,msg:'XSS'"`

6. Détection & Prévention d'Intrusion (IDS/IPS)

Type	Action	Méthodes Détection	Ex Outil
IDS	Détecte + Alerte	**Signature** (motifs connus), **Anomalie** (comportement)	Snort
IPS	Détecte + Bloque	Idem IDS (souvent intégré au PF ou WAF)	

---

7. Analyse Vulnérabilités & Logs

- **Scan Vulnérabilités :**
  Outils : Nessus, OpenVAS.
  Base : **CVE**.
  Score : **CVSS** (0-10, ex : Log4Shell 10.0).

Champ CVSS	Signification
AV	Attack Vector (N=Network, A=Adjacent, L=Local, P=Physical)
AC	Attack Complexity (L=Low, H=High)
PR	Privileges Required (N=None, L=Low, H=High)
UI	User Interaction (N=None, R=Required)
S	Scope (U=Unchanged, C=Changed)
C/I/A	Confidentiality, Integrity, Availability Impact (N=None, L=Low, H=High)

- **Logs :**
  Indispensables (Audit, Forensics).
  Surveillance : Nagios, Zabbix.

C'est un exercice de concision extrême ! J'espère que cette version très visuelle/tabulaire est ce que tu avais en tête. L'idée est d'avoir des points de repère rapides.