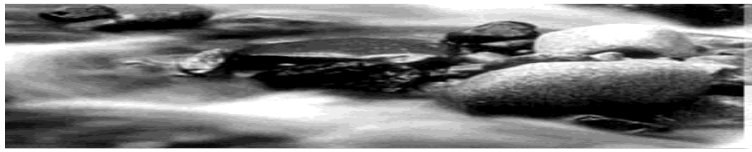
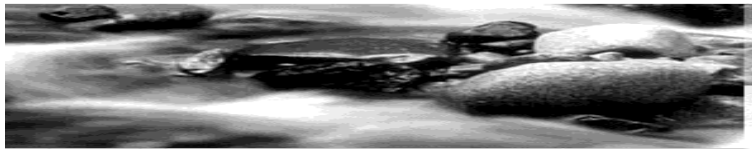


deny all
SECURITY SOLUTIONS

DENY-ALL

remote-Web



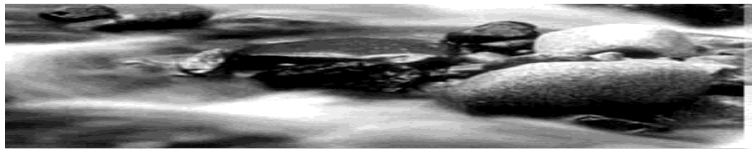
deny all
SECURITY SOLUTIONS

1 - Deny-All

- Internet & Sécurité

- Pôle produits: sécurité & contrôle applicatif
  - **rWeb**: contrôle applicatif entrant HTTP/HTTPS
  - **rFTP**: contrôle applicatif entrant FTP
  - **zProxy**: contrôle applicatif sortant HTTP(S)/FTP
  - Développement
  - Maintenance et Support

- Pôle services: expertise sécurité
  - Veille technologique sécurité
  - Assistance à MO sécurité
  - Assistance à ME sécurité

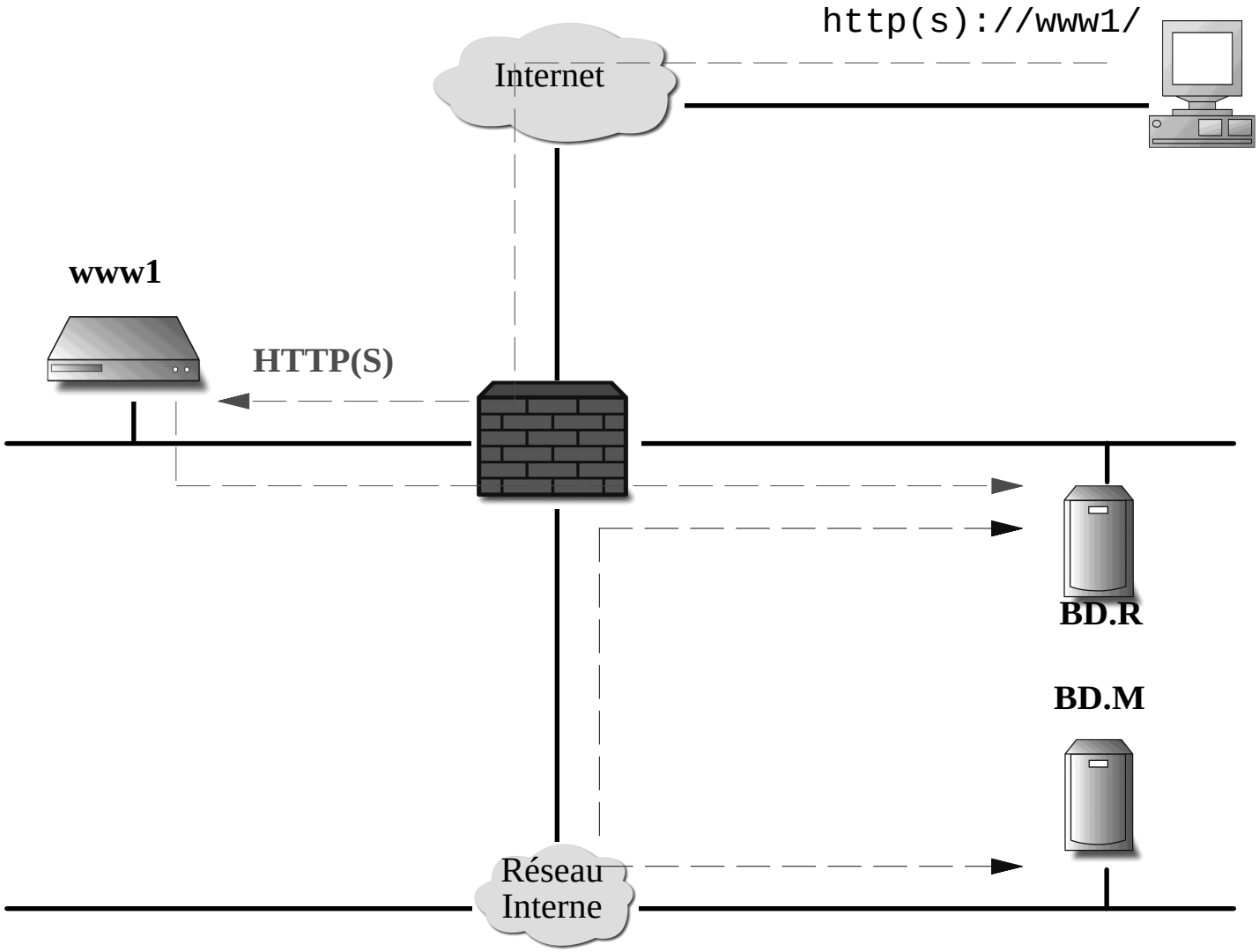


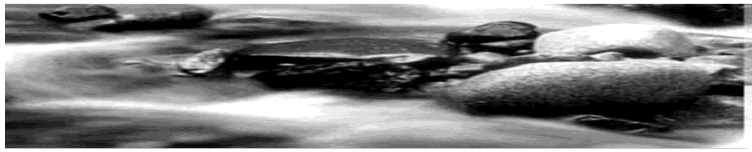
deny all
SECURITY SOLUTIONS

2 - rWeb (remote-Web)

- Robuste
  - *plusieurs années de production*
- Sécurisé
  - *développements de qualité et audit systématique*
- Performant
  - *cache, cartes accélératrices, ...*
- Simple d'utilisation
  - *administration graphique Web*
- Filtrage intégral
  - *pour chaque requête HTTP(S):*
    - URL, arguments, data
    - entêtes HTTP

3 - Architectures traditionnelles



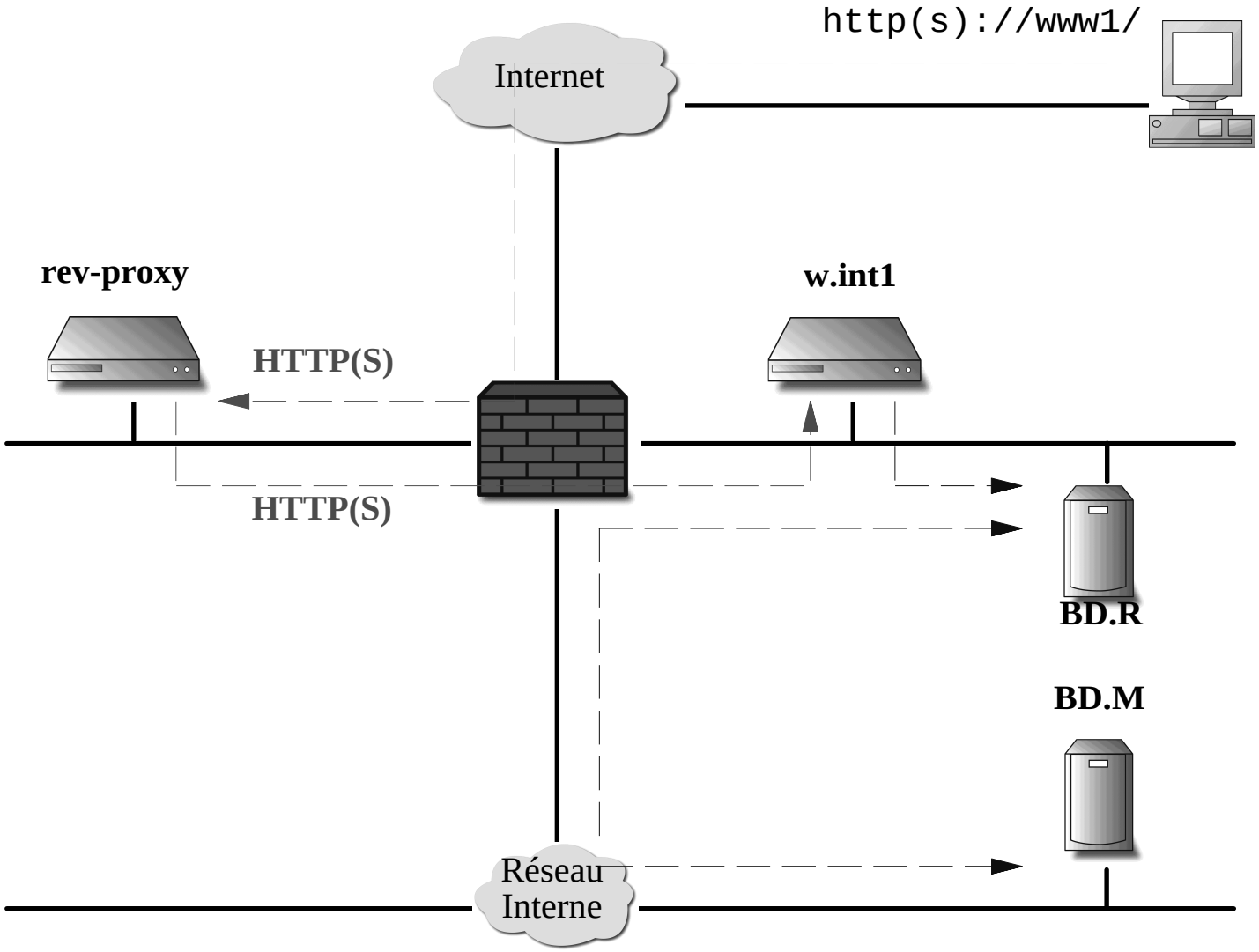


deny all
SECURITY SOLUTIONS

4 - Architectures traditionnelles

- Bugs Web !
  - `http://www/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c`
- Bugs CGI !
  - `http://www/cgi?id=314159&montant=-300`

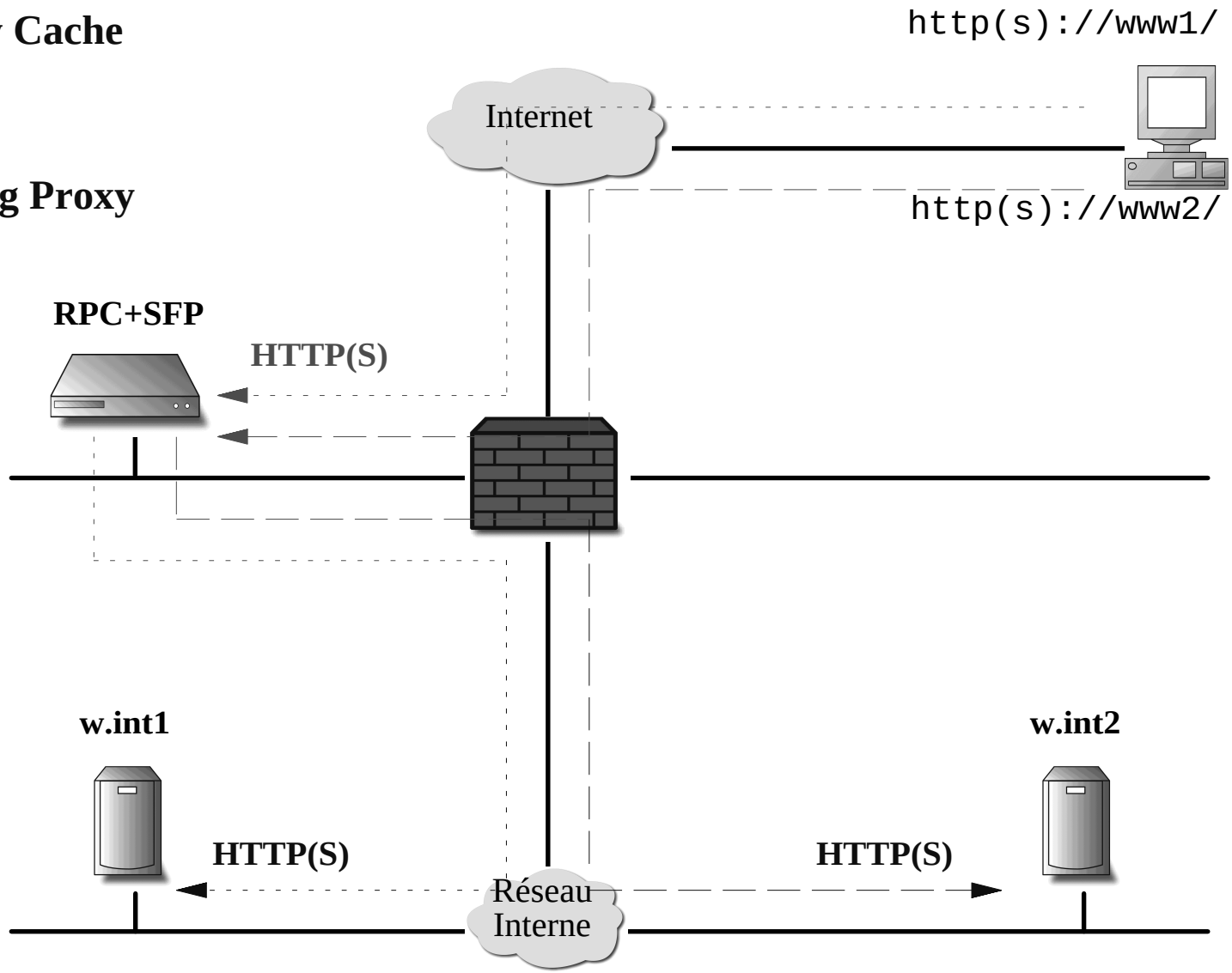
5 - Architectures reverse-proxy



6 - Architecture rWeb mono-DMZ

RPC: Reverse Proxy Cache
- présentation
- cache

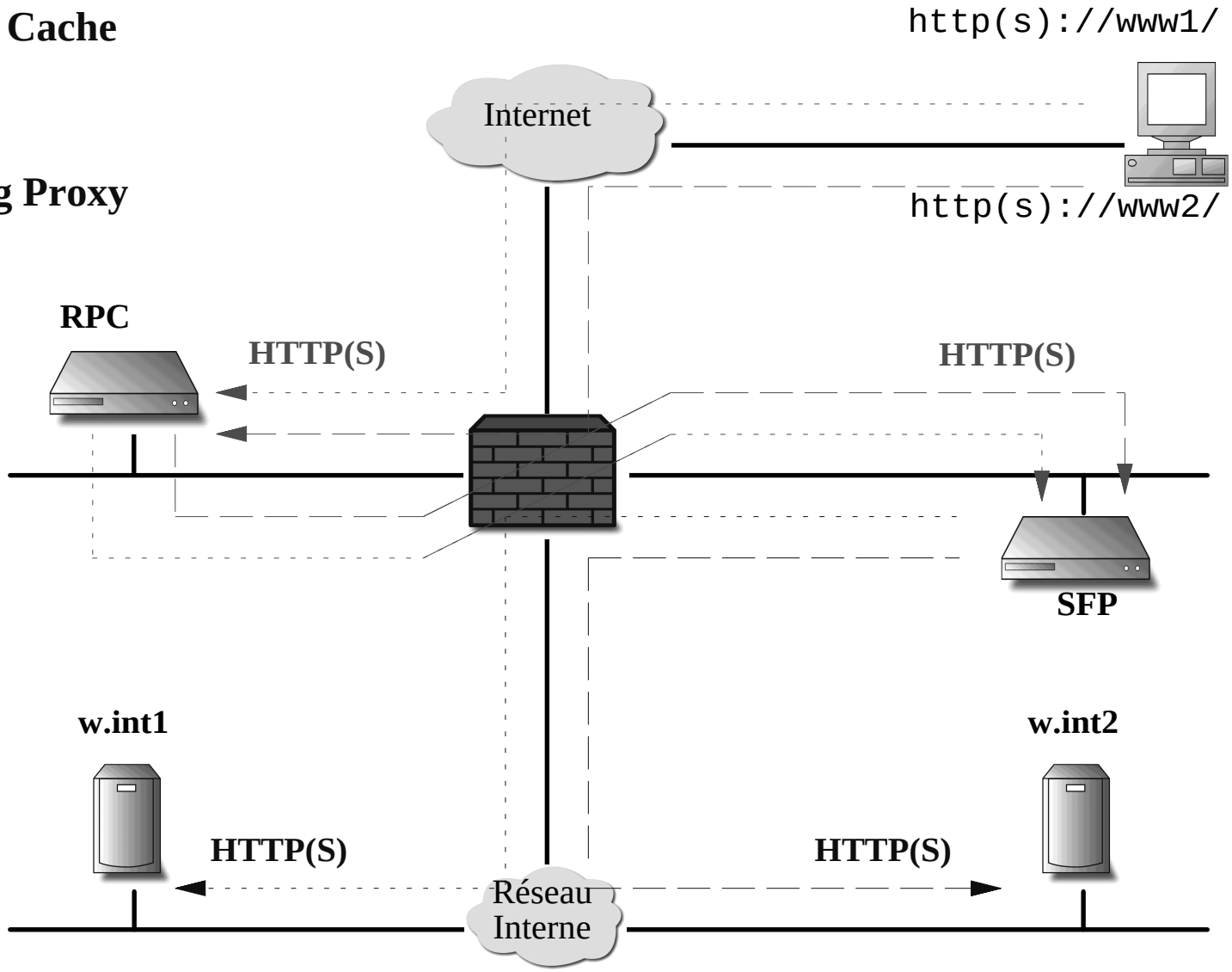
SFP: Secure Filtering Proxy
- authentification
- filtrage



7 - Architecture rWeb multi-DMZ

RPC: Reverse Proxy Cache
- présentation
- cache

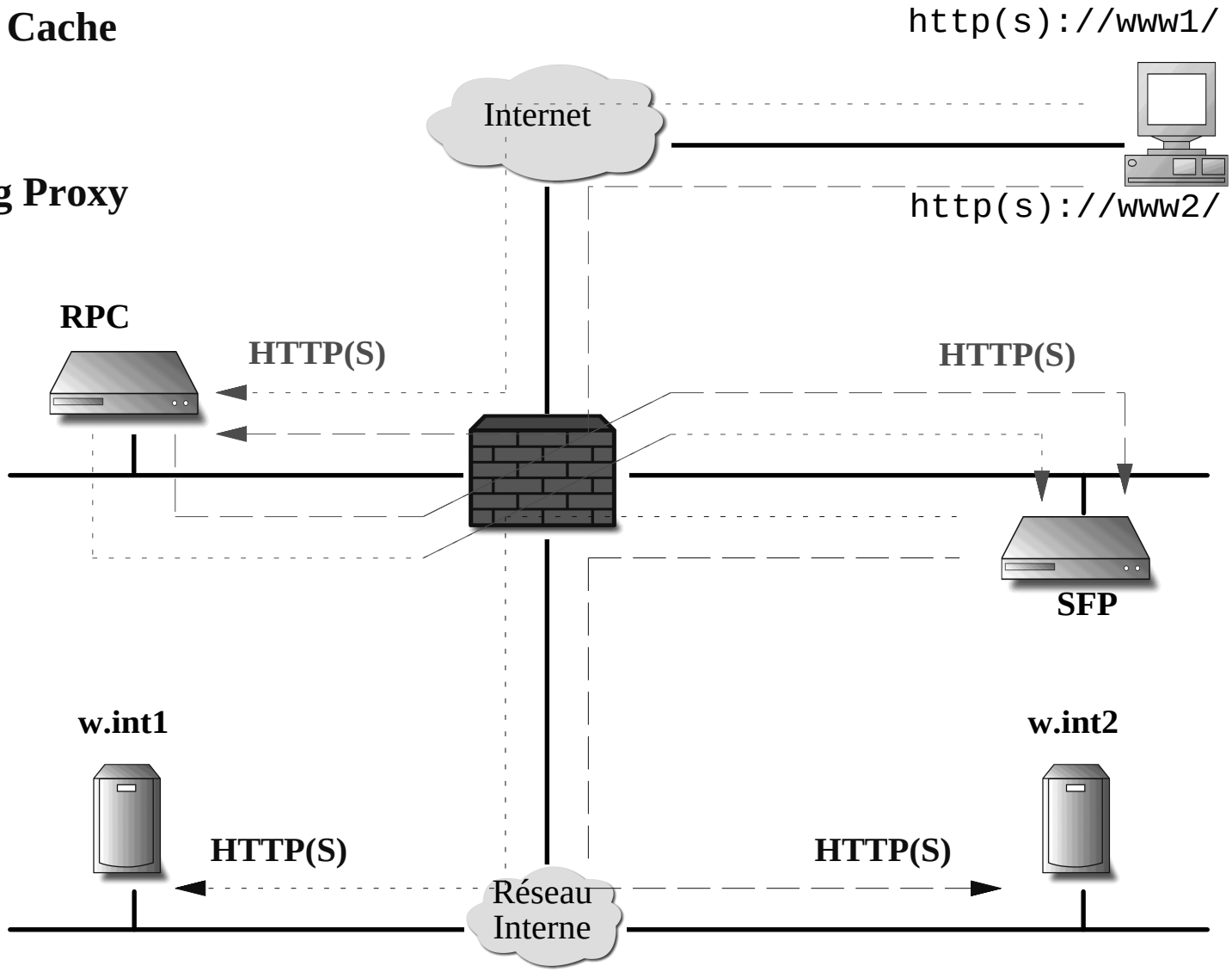
SFP: Secure Filtering Proxy
- authentification
- filtrage



8 - Architecture rWeb "pooling"

RPC: Reverse Proxy Cache
- présentation
- cache

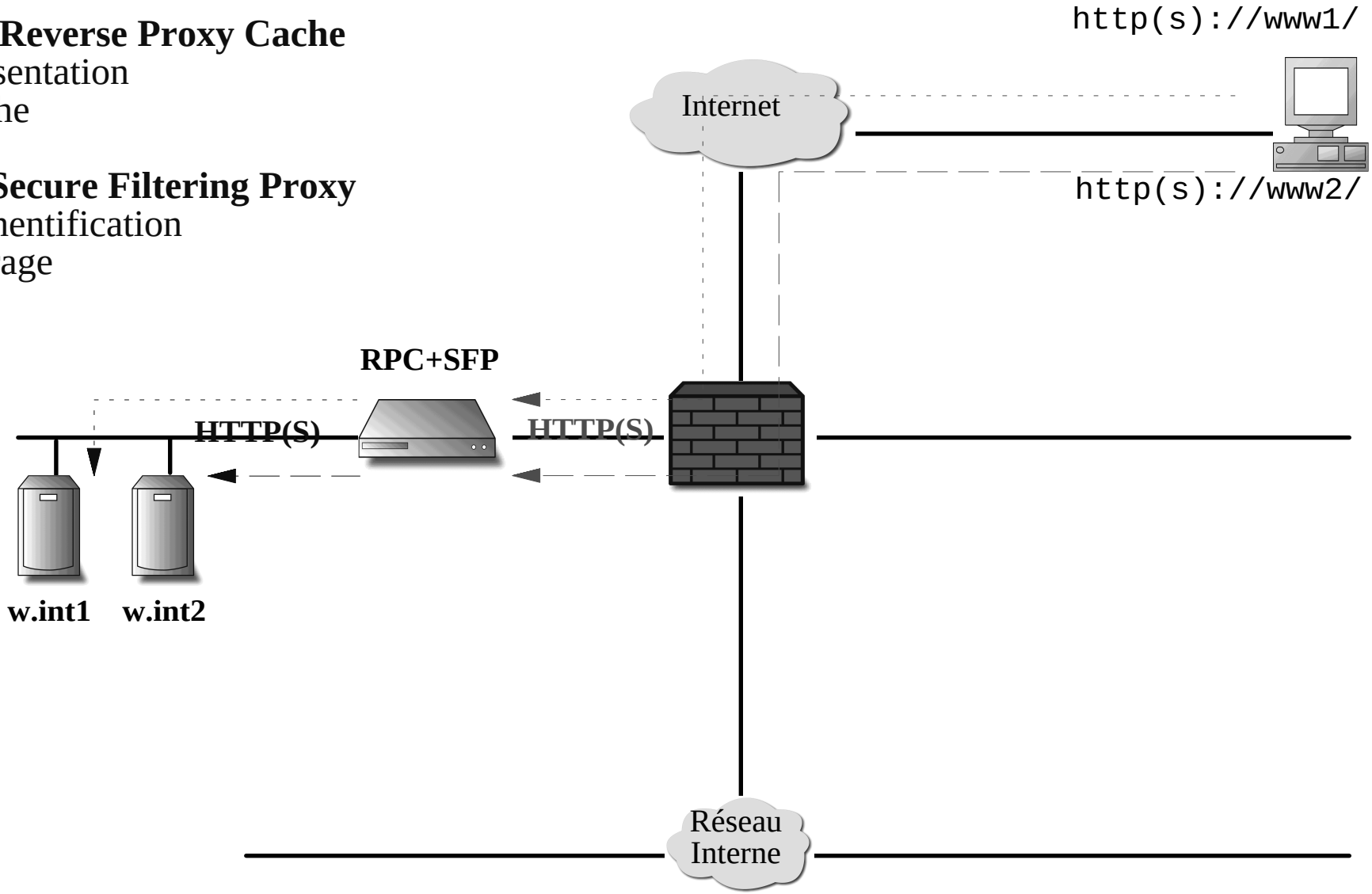
SFP: Secure Filtering Proxy
- authentification
- filtrage



9 - Architecture rWeb transparent

RPC: Reverse Proxy Cache
- présentation
- cache

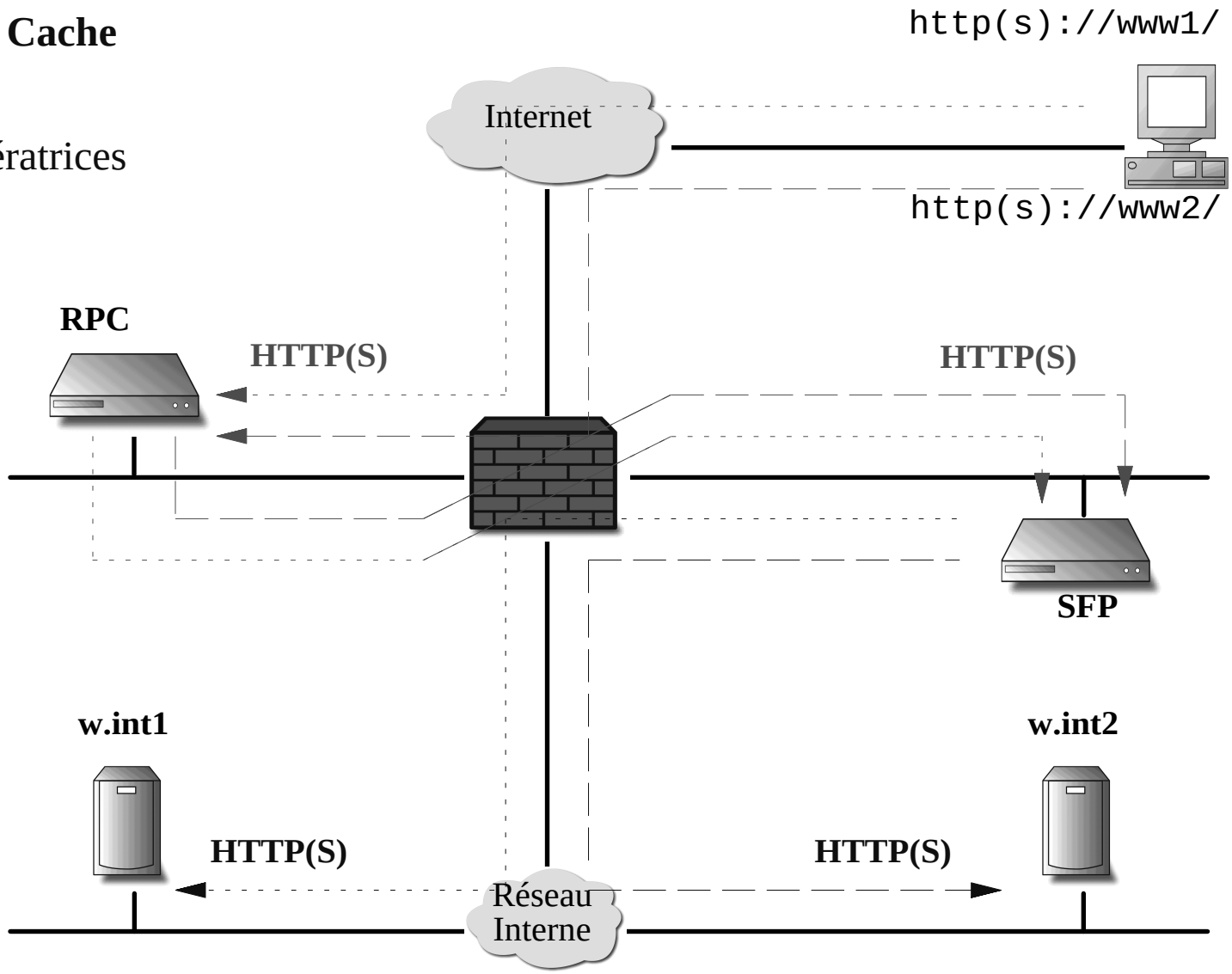
SFP: Secure Filtering Proxy
- authentification
- filtrage



10 - Architecture rWeb: RPC

RPC: Reverse Proxy Cache

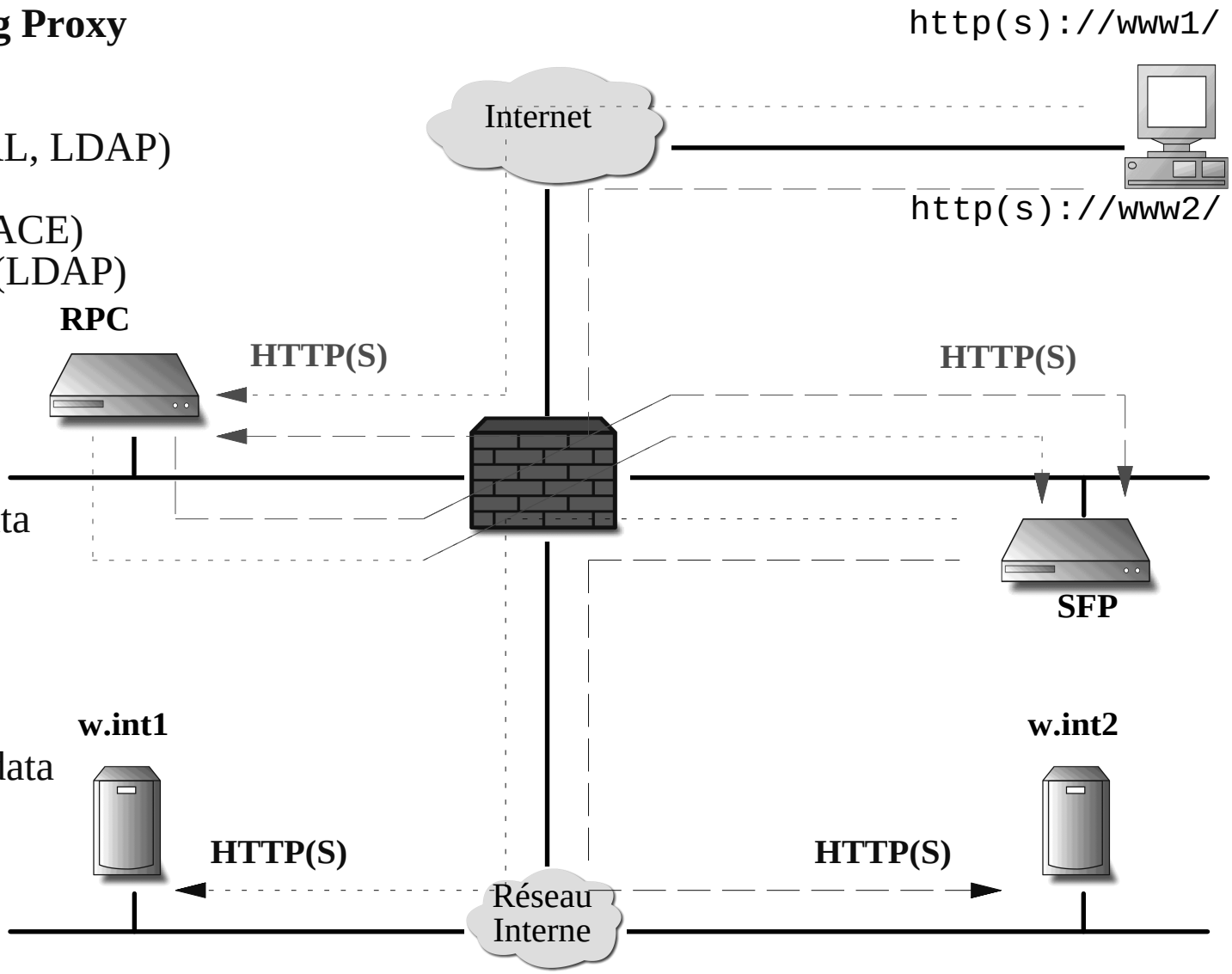
- HTTP(S) / 1.1
- SSL + cartes accélératrices
- Cache
- Compression
- Validation/Unicité des requêtes
- Traces CLF
- Relais HTTP(S)

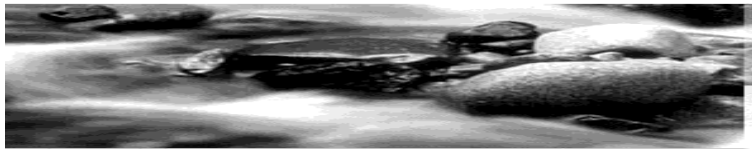


11 - Architecture rWeb: SFP

SFP: Secure Filtering Proxy

- Authentifications:
  - SSLv3 (CA, CRL, LDAP)
  - Radius
  - RSA/SecurID (ACE)
  - User/Password (LDAP)
  - ...
  - SSO
- Filtrage:
  - URI + args + data
  - entêtes HTTP
- Validation/Unicité des requêtes
- Traces URI+args+data
- Relais HTTP(S)

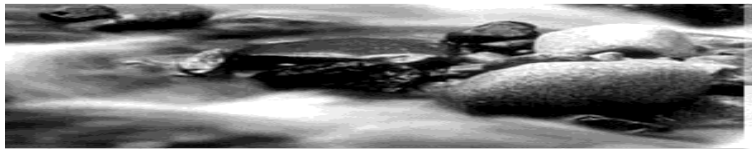




deny all
SECURITY SOLUTIONS

12 - rWeb: Filtrage

- **Automatique**
- **Assisté**
- **Outils automatiques:**
  - Validation fonctionnelle
  - Création/Vérification/Mise au point des règles de filtrage
- **Différents niveaux de filtrage**
  - "standard"
  - ...
  - "strict"



deny all
SECURITY SOLUTIONS

13 - rWeb: Filtrage "standard"

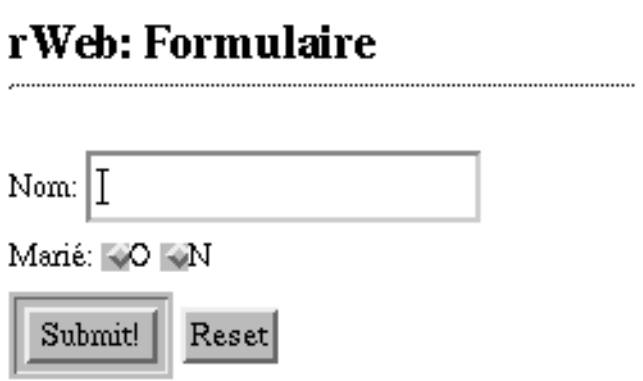
4 Principe

```
4 deny "attaque 1"
4 deny "attaque 2"
4 ...
4 permit *.html *.gif
   sans args ni data

4 permit *.jsp
   args < 1000 & data < 2000
```

14 - rWeb: Filtrage "strict"

4 Principe

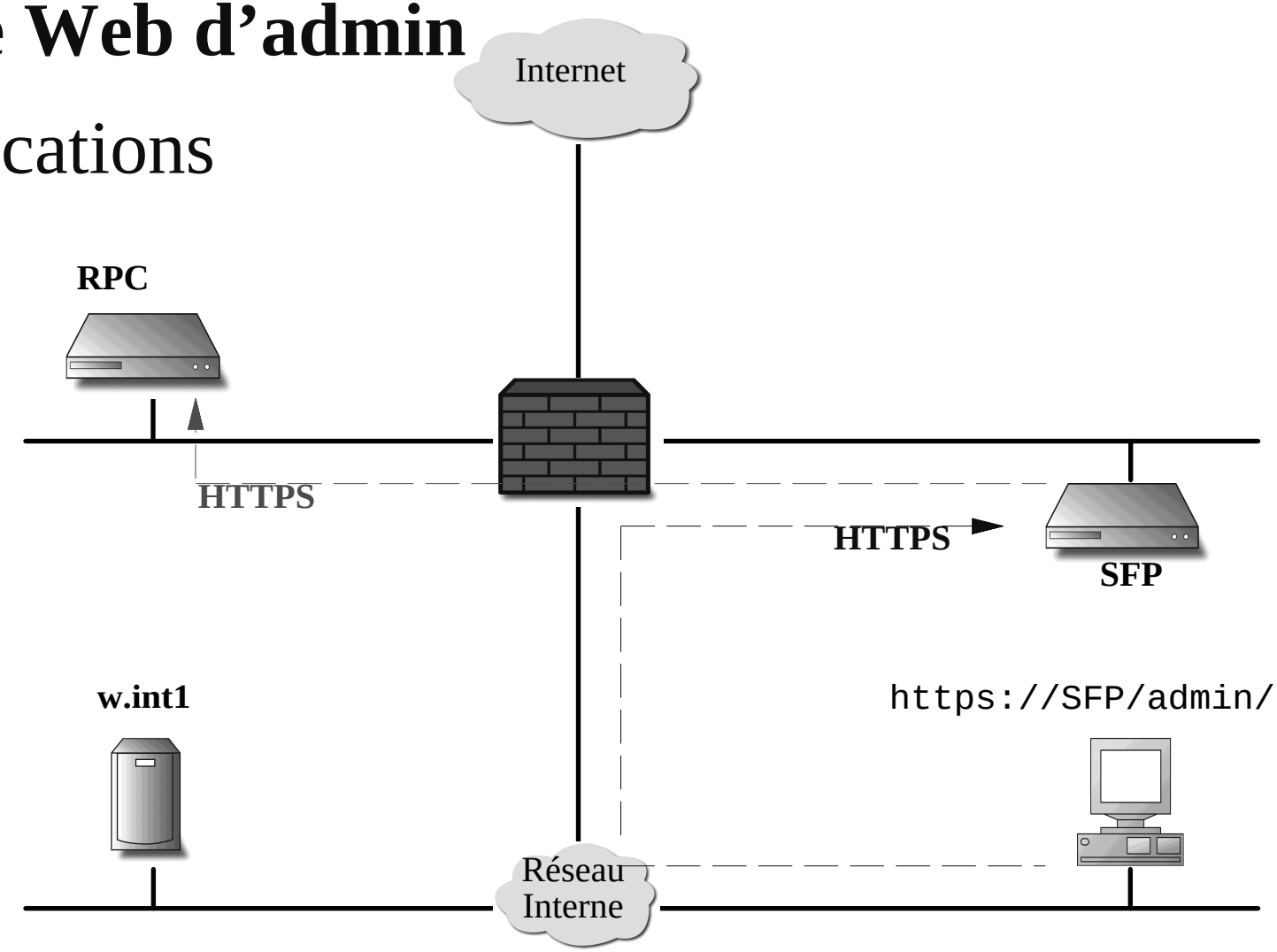



```
4 permit *.html
   sans args ni data

4 permit X.jsp
   args: -
   data: nom    : type string_32
         marie  : type boolean
4 ...
4 permit Z.jsp
   ...
```

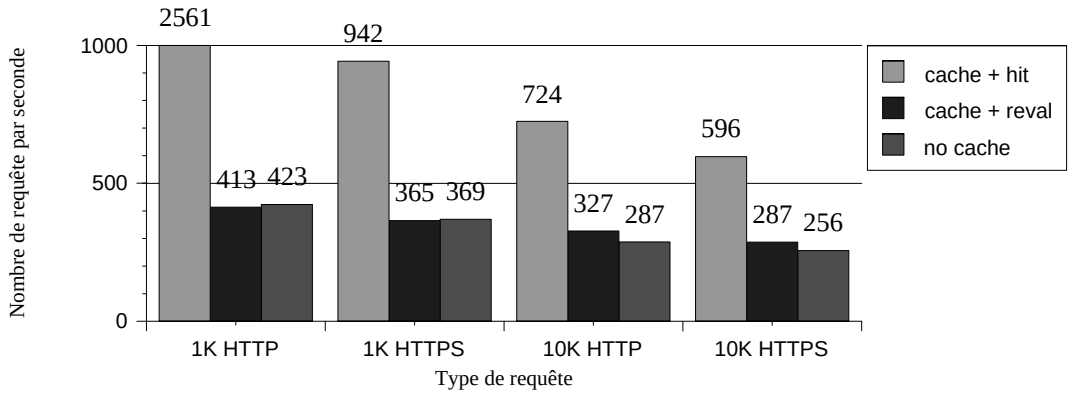
15 - Administration rWeb

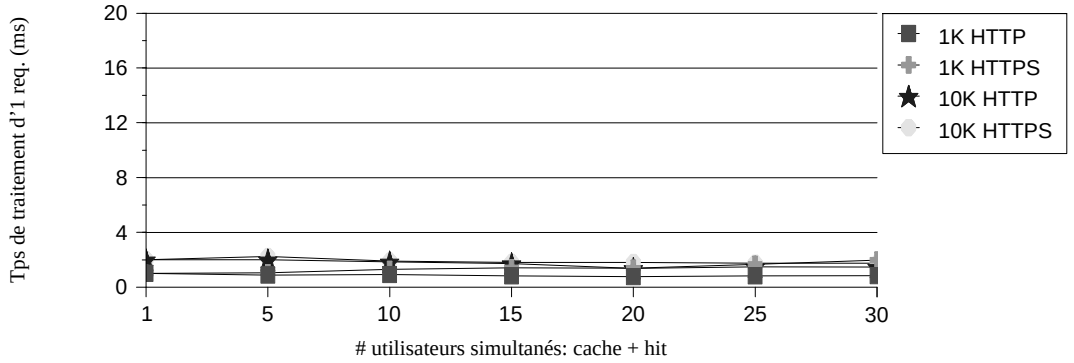
- **Interface Web d'admin**
- authentifications
- rôles
- traces
- instances
- filtrage

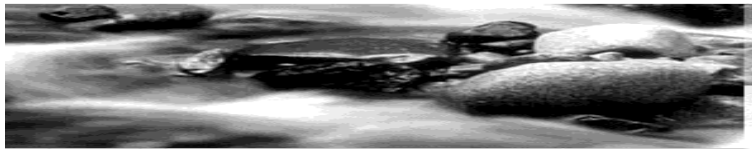


16 - Performances rWeb

4 Appliance entrée de gamme







deny all
SECURITY SOLUTIONS

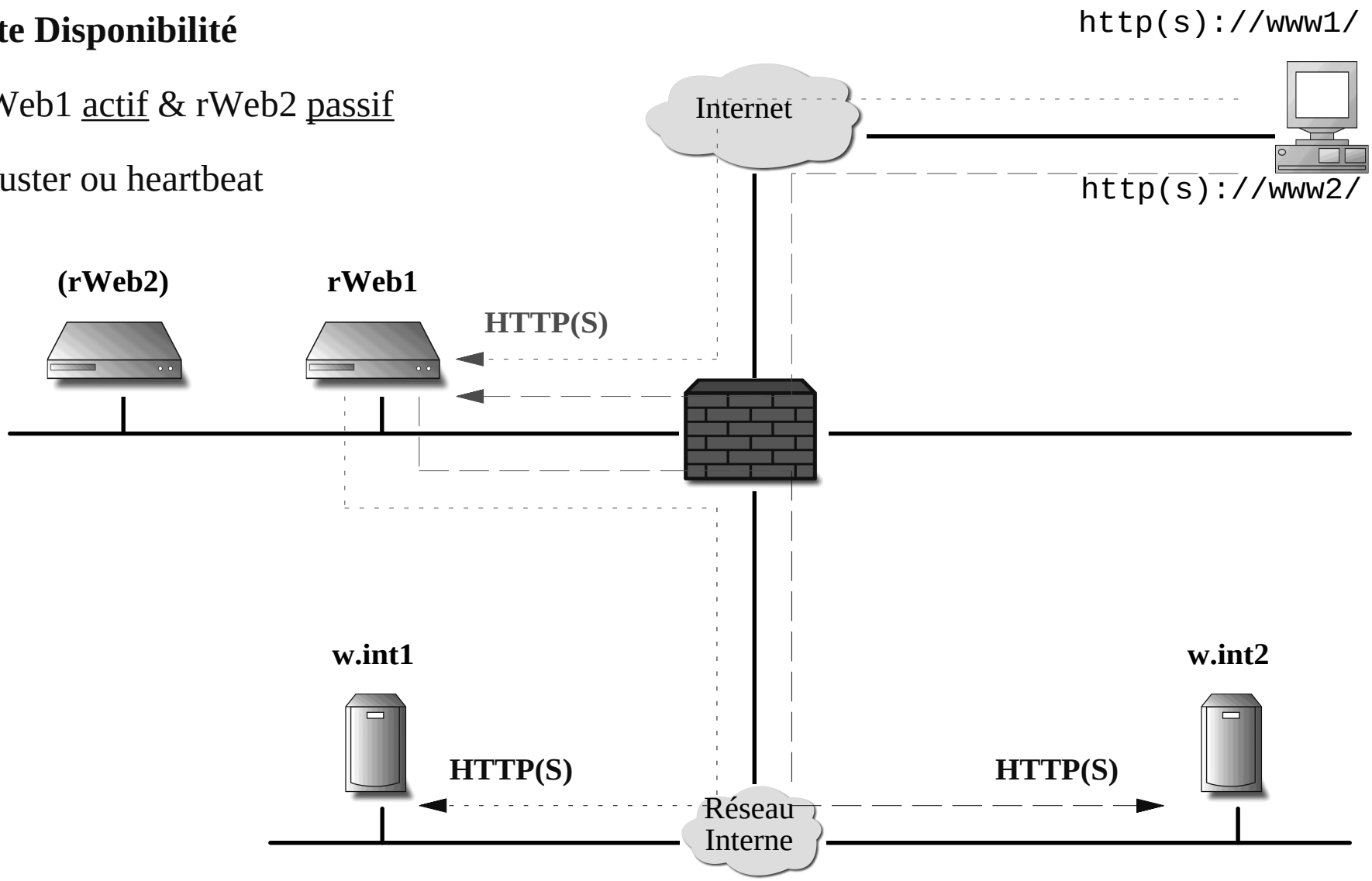
17 - Disponibilité rWeb

- **Appliance**
  - HP
  - Sun
- **Logiciel**
  - Solaris
  - Linux
  - ...

18 - HA rWeb mono-DMZ

Haute Disponibilité

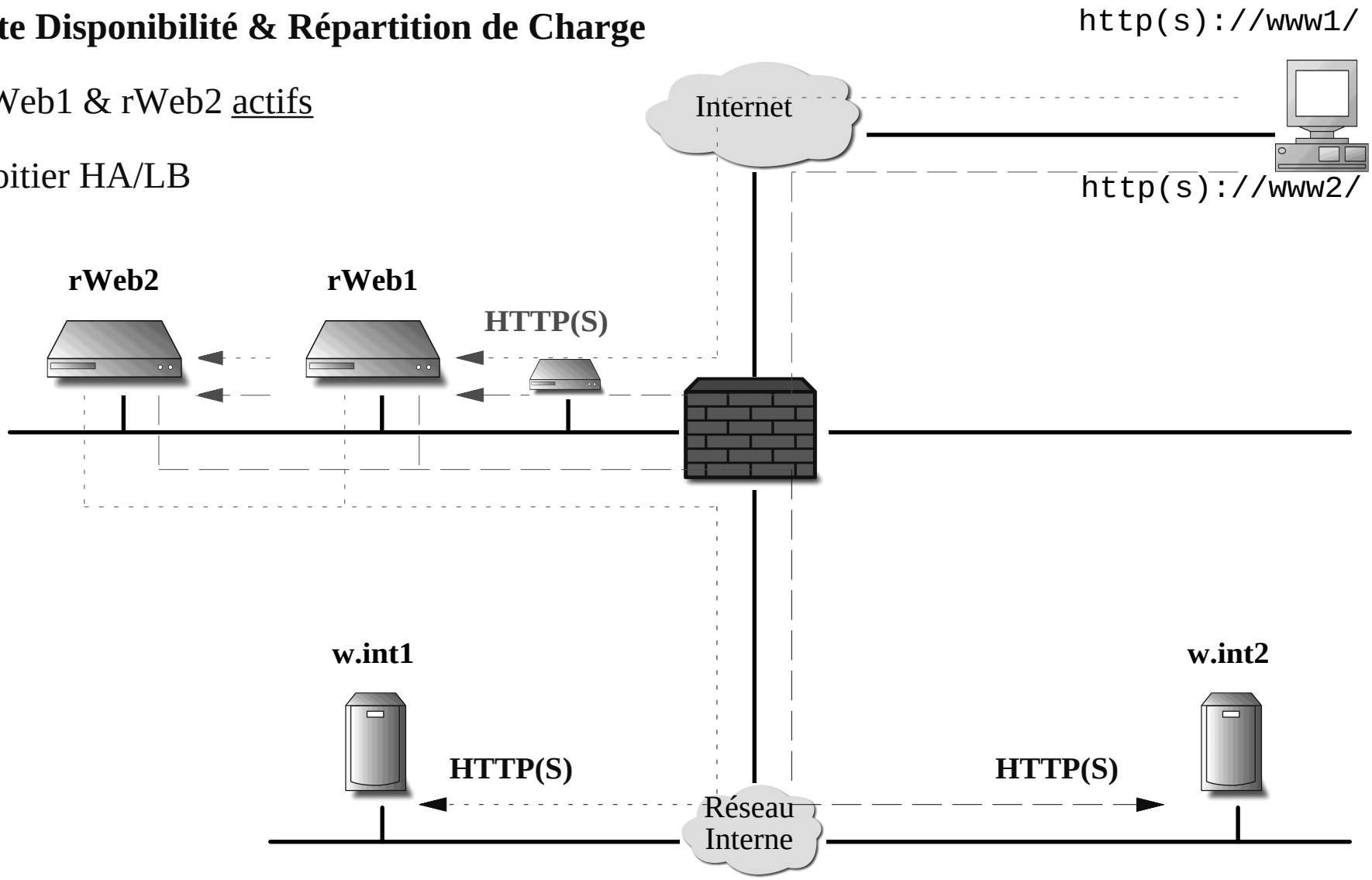
- rWeb1 actif & rWeb2 passif
- cluster ou heartbeat



19 - HA/LB rWeb mono-DMZ

Haute Disponibilité & Répartition de Charge

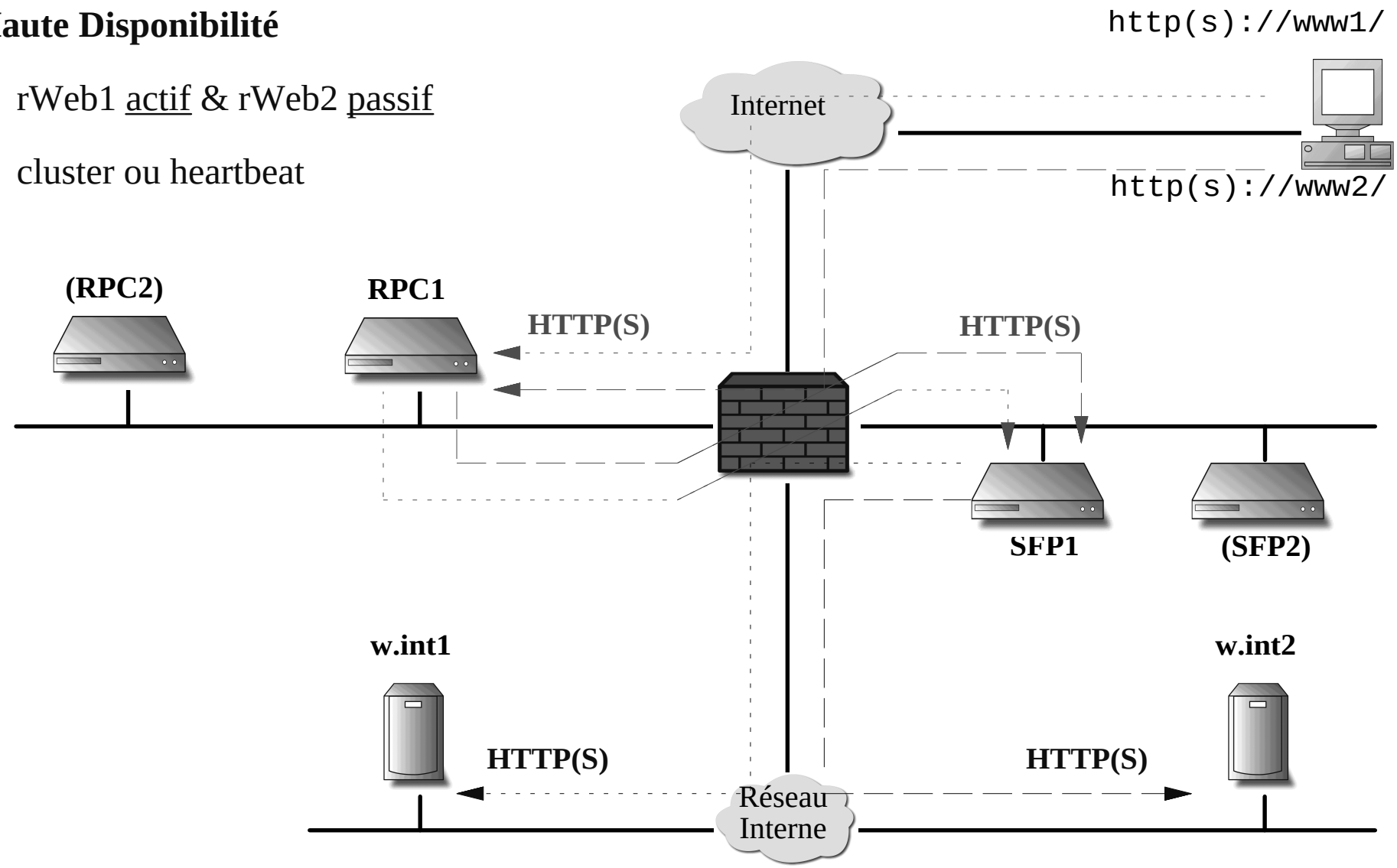
- rWeb1 & rWeb2 actifs
- boitier HA/LB



20 - HA rWeb multi-DMZ

Haute Disponibilité

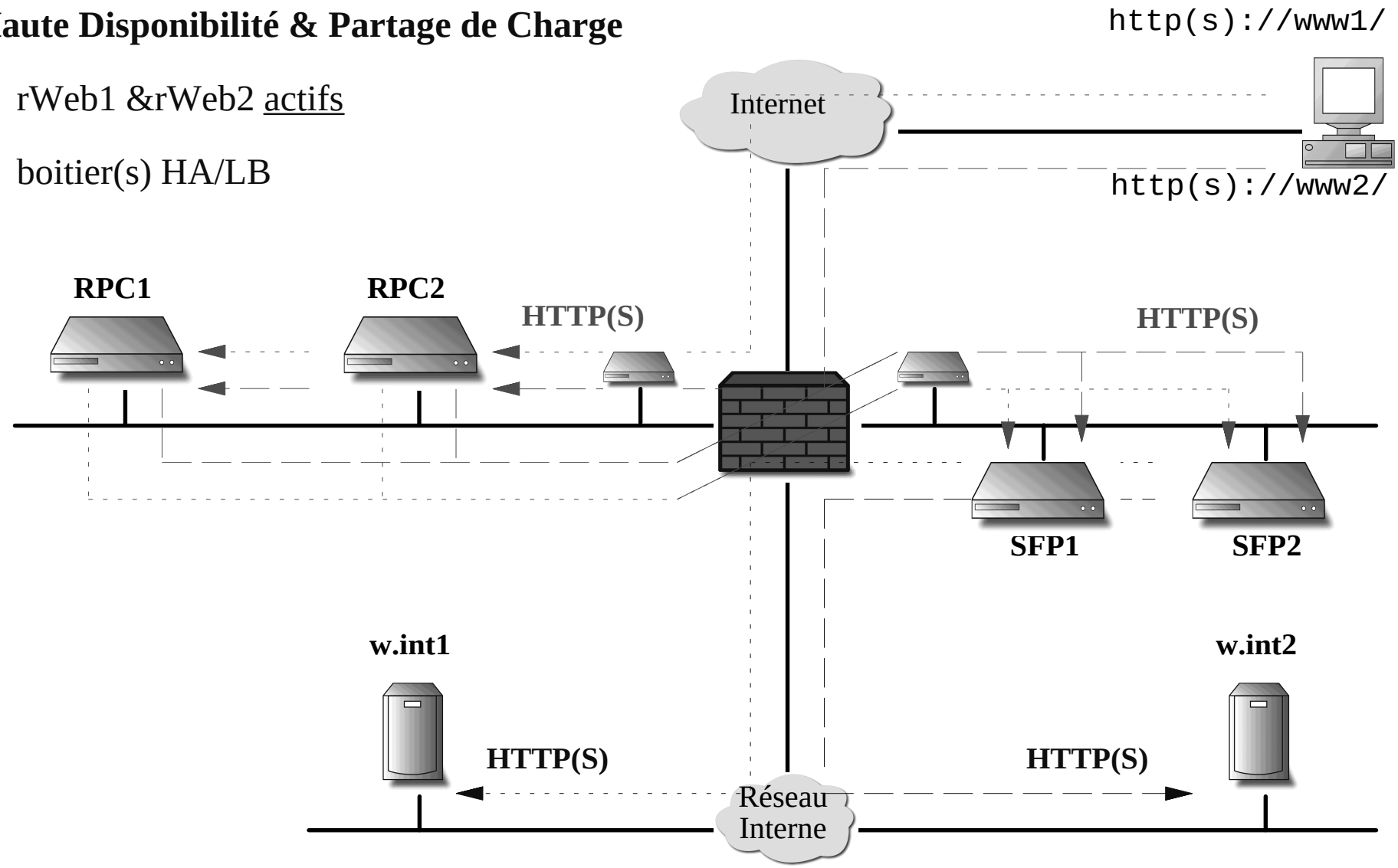
- rWeb1 actif & rWeb2 passif
- cluster ou heartbeat



21 - HA/LB rWeb multi-DMZ

Haute Disponibilité & Partage de Charge

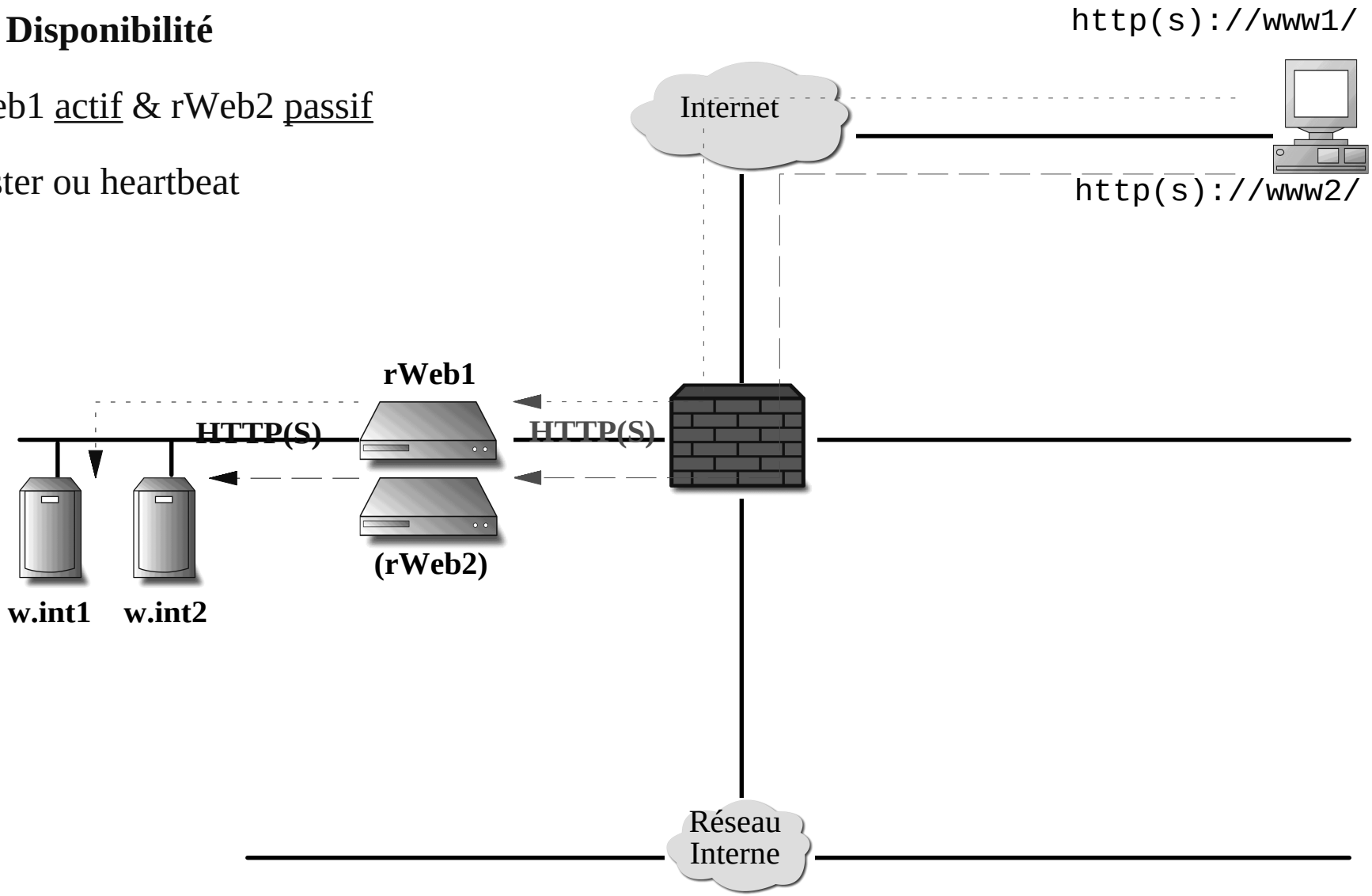
- rWeb1 &rWeb2 actifs
- boitier(s) HA/LB

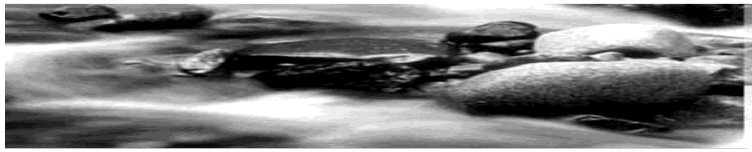


22 - HA rWeb transparent

Haute Disponibilité

- rWeb1 actif & rWeb2 passif
- cluster ou heartbeat





deny all
SECURITY SOLUTIONS

23 - Questions / Réponses