

Preuve de compétence

Épreuve E6

pfSense



Sommaire :

Concevoir une solution d'infrastructure réseau	3
1. Analyser un besoin exprimé et son contexte juridique	3
2. Étudier l'impact d'une évolution d'un élément d'infrastructure sur le système informatique	3
3. Élaborer un dossier de choix d'une solution d'infrastructure et rédiger les spécifications techniques	3
4. Maquetter et prototyper une solution d'infrastructure permettant d'atteindre la qualité de service attendue	4
5. Déterminer et préparer les tests nécessaires à la validation de la solution d'infrastructure retenue	4
Installer, tester et déployer une solution d'infrastructure réseau	6
1. Installer et configurer des éléments d'infrastructure	6
Installer et configurer le Firewall pfSense	6
Interface pfSense	7
2. Tester l'intégration et l'acceptation d'une solution d'infrastructure	10
3. Déployer une solution d'infrastructure	11

Concevoir une solution d'infrastructure réseau

1. Analyser un besoin exprimé et son contexte juridique

Le besoin exprimé était de mettre en place une infrastructure réseau sécurisée, intégrant une zone DMZ pour héberger un serveur web/FTP et un serveur messagerie accessibles depuis Internet, tout en protégeant le réseau interne de l'entreprise. Cette configuration répond à des enjeux de sécurité en séparant les services exposés du réseau local, ce qui est une bonne pratique conforme aux exigences RGPD (sécurisation des données internes).

2. Étudier l'impact d'une évolution d'un élément d'infrastructure sur le système informatique

La mise en place d'une DMZ dans l'infrastructure existante implique de revoir le plan d'adressage, le routage et les règles de filtrage entre les zones. Cela a nécessité de vérifier que l'ajout du sous-réseau 10.4.9.0/24 n'interférait pas avec les règles existantes et que les accès entre DMZ et réseau interne étaient bien contrôlés.

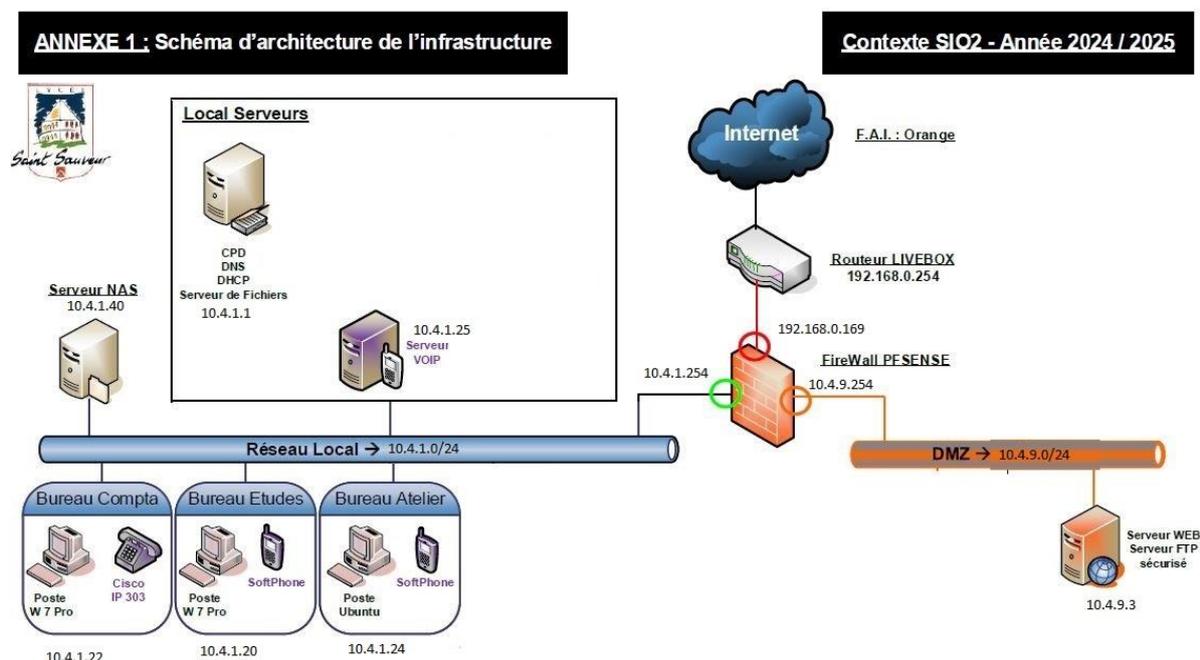
3. Élaborer un dossier de choix d'une solution d'infrastructure et rédiger les spécifications techniques

Le choix de pfSense a été motivé par sa puissance, sa flexibilité et sa compatibilité avec une DMZ multi-services. Une documentation des interfaces, du schéma réseau et firewall a été produite pour appuyer les choix techniques. Le plan d'adressage a été détaillé pour intégrer les réseaux LAN, WAN et DMZ.

4. Maquetter et prototyper une solution d'infrastructure permettant d'atteindre la qualité de service attendue

Une maquette a été réalisée dans l'environnement VMware ESXi du lycée. Elle repose sur :

- Une machine virtuelle dédiée à pfSense, avec 3 interfaces réseau configurées (WAN, LAN, OPT1/DMZ),
- Un serveur web placé dans le réseau DMZ (10.4.9.0/24),
- Des machines clientes dans le réseau LAN (10.4.1.0/24),
- Une connexion au réseau pédagogique via l'interface WAN (192.168.0.0/24).



5. Déterminer et préparer les tests nécessaires à la validation de la solution d'infrastructure retenue

Des tests ont été réalisés pour valider la séparation logique des réseaux via pfSense. Le pare-feu a été configuré avec trois interfaces distinctes (WAN, LAN et DMZ), permettant une circulation isolée entre chaque zone. pfSense agit comme point de passage entre le réseau interne, la DMZ et l'extérieur.

Une **blacklist** a été mise en place afin de bloquer l'accès à certains sites ou adresses IP depuis le réseau LAN.

Les tests effectués ont permis de vérifier :

- la connectivité de base entre les zones,
- le bon fonctionnement de l'accès à Internet depuis le LAN,
- et l'application correcte de la blacklist configurée dans l'interface de filtrage de pfSense.

Installer, tester et déployer une solution d'infrastructure réseau

1. Installer et configurer des éléments d'infrastructure

Le firewall pfSense a été installé et configuré avec trois interfaces :

- WAN (192.168.0.169),
- LAN (10.4.1.254),
- OPT1/DMZ (10.4.9.254).

Les adresses IP ont été attribuées, le routage activé, et les services DNS, NAT et firewall ont été configurés.

Installer et configurer le Firewall pfSense

Suivre l'installation et au moment de reboot, il faut éjecter virtuellement le disque pour ne pas redémarrer la configuration.

On arrive sur cette page:

```
WAN (wan)      -> vmx1      -> v4: 192.168.0.169/24
LAN (lan)      -> vmx0      -> v4: 10.4.1.254/24
OPT1 (opt1)    -> vmx2      -> v4: 10.4.9.254/24
```

Où on configure l'entrée WAN, en accès par pont vers le réseau de la salle, ici en avec 192.168.0.168.

Puis on ajoute un LAN, qui mènera vers les machines du réseau Littoral 10.4.1.0/24, on le met en 10.4.1.254/24, qui sera le gateway des machines dans ce réseau.

Puis on ajoute un OPT1, qui mènera vers le réseau de 10.4.9.0/24, qui sera le réseau de la DMZ, avec l'ip 10.4.9.254, qui sera leur gateway.

Interface pfSense

The screenshot shows the pfSense web interface. At the top left, the IP address 10.4.1.254 is highlighted in a red box. The navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. A warning message is displayed: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' Below this, the 'Status / Dashboard' section is visible. The 'System Information' panel on the left provides details about the system, including the name 'pfSense.home.arpa', user 'admin@10.4.1.20', system type 'VMware Virtual Machine', BIOS vendor 'Phoenix Technologies LTD', and version '2.7.2-RELEASE (amd64)'. The 'Netgate Services And Support' panel on the right shows the contract type as 'Community Support' and provides links to support resources. At the bottom right, the 'Interfaces' panel is highlighted with a red box, showing three interfaces: WAN (192.168.0.169), LAN (10.4.1.254), and OPT1 (10.4.9.254).

Ainsi on arrive sur cette interface, si on rentre l'ip du gateway pour le réseau 10.4.1.0 (on peut faire pareil du coté OPT1 ou WAN avec leurs interfaces respectives)

On retrouve en bas à droite toutes les interfaces du pfSense.

Activer la black list

The screenshot shows the 'Services' menu in the pfSense interface. The 'VPN' sub-menu is selected. The following services are listed: Auto Config Backup, Captive Portal, DHCP Relay, DHCP Server, DHCPv6 Relay, DHCPv6 Server, DNS Forwarder, DNS Resolver, Dynamic DNS, IGMP Proxy, NRPE, NTP, PPPoE Server, Router Advertisement, SNMP, Squid Proxy Server, Squid Reverse Proxy, SquidGuard Proxy Filter, UPnP & NAT-PMP, and Wake-on-LAN. The 'Squid Proxy Server', 'Squid Reverse Proxy', and 'SquidGuard Proxy Filter' options are highlighted with red boxes.

Il faut aller dans les options de Squidguard

General settings Common ACL Groups ACL Target categories Times Rewrites **Blacklist** Log XMLRPC Sync

Blacklist Update

0%

Enter FTP or HTTP path to the blacklist archive here.

Blacklist update Log

```

Begin blacklist update
Start download.
Download archive http://dsi.ut-capitole.fr/blacklists/download
/blacklists_for_pfsense.tar.gz
Download complete
Unpack archive
Scan blacklist categories.
Found 68 items.
Start rebuild DB.
Copy DB to workdir.
Reconfigure Squid proxy.
Blacklist update complete.

```

Ensuite importer la black list de l'université de Toulouse.

General settings Common ACL Groups ACL Target categories Times Rewrites **Blacklist** Log XMLRPC Sync

General Options

Enable Check this option to enable squidGuard.
 Important: Please set up at least one category on the 'Target Categories' tab before enabling. See [this link for details](#).
 The Save button at the bottom of this page must be clicked to save configuration changes.
 To activate squidGuard configuration changes, **the Apply button must be clicked.**

SquidGuard service state: **STARTED**

Activer Squidguard

Target Rules List

ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

Target Categories

[oui]	access	deny	▼
[blk_blacklists_adult]	access	deny	▼
[blk_blacklists_agressif]	access	deny	▼
[blk_blacklists_arjel]	access	deny	▼
[blk_blacklists_associations_religieuses]	access	deny	▼
[blk_blacklists_astrology]	access	deny	▼
[blk_blacklists_audio-video]	access	deny	▼
[blk_blacklists_bank]	access	deny	▼
[blk_blacklists_bitcoin]	access	deny	▼
[blk_blacklists_blog]	access	deny	▼
[blk_blacklists_celebrity]	access	deny	▼
[blk_blacklists_chat]	access	deny	▼
[blk_blacklists_child]	access	deny	▼
[blk_blacklists_cleaning]	access	deny	▼
[blk_blacklists_cooking]	access	deny	▼
[blk_blacklists_cryptojacking]	access	deny	▼
[blk_blacklists_dangerous_material]	access	deny	▼
[blk_blacklists_dating]	access	deny	▼
[blk_blacklists_ddos]	access	deny	▼
[blk_blacklists_diafer]	access	deny	▼
[blk_blacklists_doh]	access	deny	▼
[blk_blacklists_download]	access	deny	▼
[blk_blacklists_drogue]	access	deny	▼
[blk_blacklists_dynamic-dns]	access	deny	▼
[blk_blacklists_educational_games]	access	deny	▼
[blk_blacklists_evemen_pix]	access	deny	▼
[blk_blacklists_exceptions_liste_bu]	access	deny	▼
[blk_blacklists_fakenews]	access	deny	▼
[blk_blacklists_filehosting]	access	deny	▼

Puis refuser tous les termes de la black list.

2. Tester l'intégration et l'acceptation d'une solution d'infrastructure

Des tests de connexion ont été réalisés depuis :

- Le reseau Littoral (10.4.1.0/24) à la DMZ (10.4.9.0/24) et de Littoral à internet :

```
C:\Users\Chillb2>ping 10.4.9.1
Envoi d'une requête 'Ping' 10.4.9.1 avec 32 octets de données :
Réponse de 10.4.9.1 : octets=32 temps<1ms TTL=63

Statistiques Ping pour 10.4.9.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Chillb2>ping 8.8.8.8
Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=7 ms TTL=109
Réponse de 8.8.8.8 : octets=32 temps=10 ms TTL=109
Réponse de 8.8.8.8 : octets=32 temps=7 ms TTL=109
Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=109

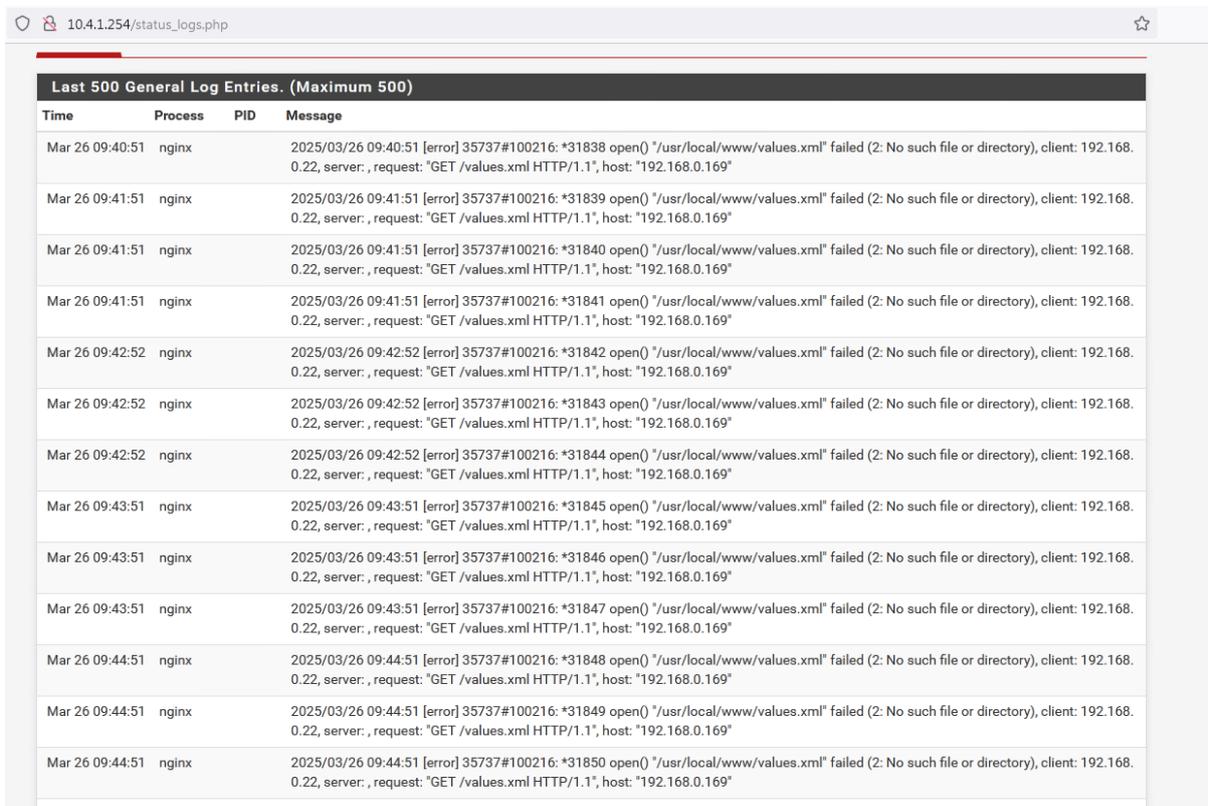
Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 7ms, Maximum = 10ms, Moyenne = 8ms
```

- DMZ vers internet :

```
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_code1 state UP group default qlen 100
0
    link/ether 00:50:56:bf:90:75 brd ff:ff:ff:ff:ff:ff
    inet 10.4.9.1/24 brd 10.4.9.255 scope global ens160
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:febf:9075/64 scope link
        valid_lft forever preferred_lft forever
root@messagerie:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=109 time=11.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=109 time=8.77 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=109 time=8.09 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 8.094/9.567/11.842/1.631 ms
```

3. Déployer une solution d'infrastructure

La solution a été déployée sur une machine virtuelle dédiée au firewall pfSense, intégrée à l'environnement ESXi. Le serveur web/FTP a été mis en ligne dans la DMZ , et l'ensemble a été documenté pour permettre un déploiement fiable et reproductible.



The screenshot shows a web browser window with the address bar containing '10.4.1.254/status_logs.php'. The main content area displays a table titled 'Last 500 General Log Entries. (Maximum 500)'. The table has four columns: 'Time', 'Process', 'PID', and 'Message'. The messages in the table are identical, indicating a series of failed GET requests to '/values.xml' from the client IP 192.168.0.22 to the server IP 192.168.0.169. The errors are caused by a '2: No such file or directory' condition.

Time	Process	PID	Message
Mar 26 09:40:51	nginx		2025/03/26 09:40:51 [error] 35737#100216: *31838 open() "/usr/local/www/values.xml" failed (2: No such file or directory), client: 192.168.0.22, server: , request: "GET /values.xml HTTP/1.1", host: "192.168.0.169"
Mar 26 09:41:51	nginx		2025/03/26 09:41:51 [error] 35737#100216: *31839 open() "/usr/local/www/values.xml" failed (2: No such file or directory), client: 192.168.0.22, server: , request: "GET /values.xml HTTP/1.1", host: "192.168.0.169"
Mar 26 09:41:51	nginx		2025/03/26 09:41:51 [error] 35737#100216: *31840 open() "/usr/local/www/values.xml" failed (2: No such file or directory), client: 192.168.0.22, server: , request: "GET /values.xml HTTP/1.1", host: "192.168.0.169"
Mar 26 09:41:51	nginx		2025/03/26 09:41:51 [error] 35737#100216: *31841 open() "/usr/local/www/values.xml" failed (2: No such file or directory), client: 192.168.0.22, server: , request: "GET /values.xml HTTP/1.1", host: "192.168.0.169"
Mar 26 09:42:52	nginx		2025/03/26 09:42:52 [error] 35737#100216: *31842 open() "/usr/local/www/values.xml" failed (2: No such file or directory), client: 192.168.0.22, server: , request: "GET /values.xml HTTP/1.1", host: "192.168.0.169"
Mar 26 09:42:52	nginx		2025/03/26 09:42:52 [error] 35737#100216: *31843 open() "/usr/local/www/values.xml" failed (2: No such file or directory), client: 192.168.0.22, server: , request: "GET /values.xml HTTP/1.1", host: "192.168.0.169"
Mar 26 09:42:52	nginx		2025/03/26 09:42:52 [error] 35737#100216: *31844 open() "/usr/local/www/values.xml" failed (2: No such file or directory), client: 192.168.0.22, server: , request: "GET /values.xml HTTP/1.1", host: "192.168.0.169"
Mar 26 09:43:51	nginx		2025/03/26 09:43:51 [error] 35737#100216: *31845 open() "/usr/local/www/values.xml" failed (2: No such file or directory), client: 192.168.0.22, server: , request: "GET /values.xml HTTP/1.1", host: "192.168.0.169"
Mar 26 09:43:51	nginx		2025/03/26 09:43:51 [error] 35737#100216: *31846 open() "/usr/local/www/values.xml" failed (2: No such file or directory), client: 192.168.0.22, server: , request: "GET /values.xml HTTP/1.1", host: "192.168.0.169"
Mar 26 09:43:51	nginx		2025/03/26 09:43:51 [error] 35737#100216: *31847 open() "/usr/local/www/values.xml" failed (2: No such file or directory), client: 192.168.0.22, server: , request: "GET /values.xml HTTP/1.1", host: "192.168.0.169"
Mar 26 09:44:51	nginx		2025/03/26 09:44:51 [error] 35737#100216: *31848 open() "/usr/local/www/values.xml" failed (2: No such file or directory), client: 192.168.0.22, server: , request: "GET /values.xml HTTP/1.1", host: "192.168.0.169"
Mar 26 09:44:51	nginx		2025/03/26 09:44:51 [error] 35737#100216: *31849 open() "/usr/local/www/values.xml" failed (2: No such file or directory), client: 192.168.0.22, server: , request: "GET /values.xml HTTP/1.1", host: "192.168.0.169"
Mar 26 09:44:51	nginx		2025/03/26 09:44:51 [error] 35737#100216: *31850 open() "/usr/local/www/values.xml" failed (2: No such file or directory), client: 192.168.0.22, server: , request: "GET /values.xml HTTP/1.1", host: "192.168.0.169"