



Formation OpenClassrooms Administrateur Systèmes, Réseaux Et Sécurité

Soutenance Projet-05

Stéphane Perfetti

20/06/2024

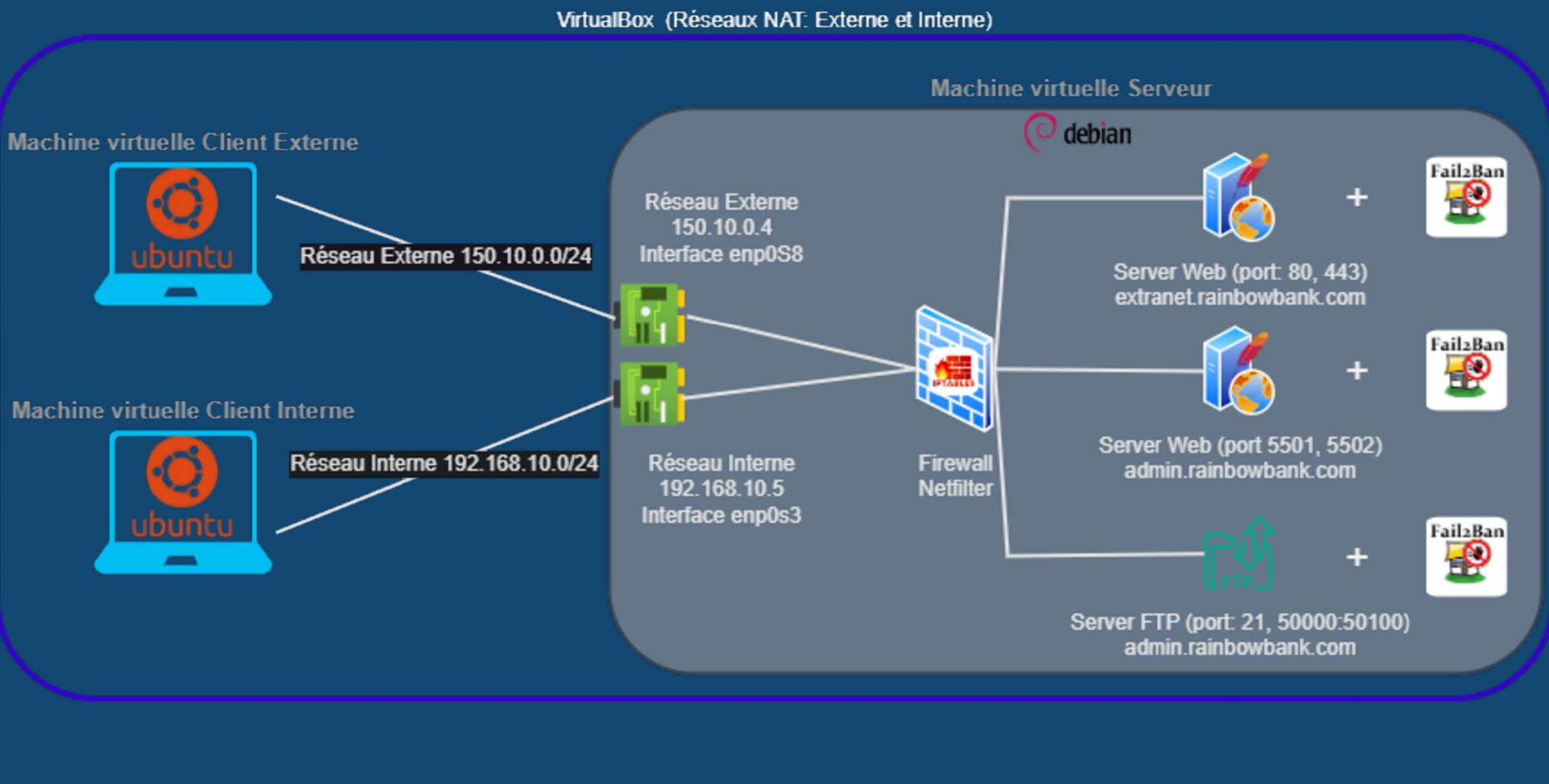


Projet 05

-
Mettez en place
des services web
sécurisés

- Scénario :
 - La société Rainbow Bank, souhaite déployer un service extranet.
 - Mission: créer un prototype opérationnel de l'infrastructure.
- Plan d'action :
 - Schéma de l'architecture du prototype
 - Serveurs web et configuration
 - Service FTP et configuration
 - Filtrage IP et outil de bannissement

Architecture du prototype



Serveurs web arborescence:

```
debian@P05Debian ~ ➔ ll --tree --level=2 --no-time /var/www/rainbowbank
Permissions Size User Group Name
drwxrwx--- - www-data www-data /var/www/rainbowbank
drwxrwx--- - www-data www-data admin.rainbowbank.com
drwxrwx--- - www-data www-data css
drwxrwx--- - www-data www-data favicon.ico
drwxrwx--- - www-data www-data images
drwxrwx--- - www-data www-data index.html
drwxrwx--- - www-data www-data js
drwxrwx--- - www-data www-data pdf
drwxrwx-W- - www-data www-data extranet.rainbowbank.com
drwxrwx--- - www-data www-data css
drwxrwx--- - www-data www-data favicon.ico
drwxrwx--- - www-data www-data images
drwxrwx--- - www-data www-data index.html
drwxrwx--- - www-data www-data js
drwxrwx--- - www-data www-data pdf
drwxrwx--- - www-data www-data images-sites
drwxrwx--- - www-data www-data images-admin
drwxrwx--- - www-data www-data images-extranet
drwxrwx--- - www-data www-data log
drwxrwx--- - www-data www-data apache_access_admin.log
drwxrwx--- - www-data www-data apache_access_extranet.log
drwxrwx--- - www-data www-data apache_error.log
drwxrwx--- - www-data www-data apache_mod-evasive
drwxrwx--- - www-data www-data nginx_access_admin.log
drwxrwx--- - www-data www-data nginx_access_extranet.log
drwxrwx--- - www-data www-data nginx_error.log
drwxrwx--- - www-data www-data TLS Certificat
drwxrwx--- - www-data www-data CA
drwxrwx--- - www-data www-data self-signed
```

- Racine des serveurs web sous: /var/www/rainbowbank/
 - admin.rainbowbank.com: site d'administration extranet
 - extranet.rainbowbank.com: site extranet
 - images-sites: montage par fstab des répertoires images des deux sites dans le répertoire images-sites.
 - log: regroupe les fichiers logs en fonction du service web.
 - *_error.log, fichier commun aux deux sites.
 - *_access_*.log, fichiers de connexion pour chaque site.
 - apache_mod-evasive, fichier log du module apache evasive.
 - TLS_certificat: regroupe les certificats et clés TLS.
 - CA: fichiers pour la ICP (PKI) du site admin.rainbowbank.com.
 - self-signed: fichiers du site extranet.rainbowbank.com
- Dossiers, propriété et droits:
 - Propriété de l'utilisateur système www-data, groupe www-data.
 - Droits de lecture, écriture et exécution pour l'utilisateur et le groupe utilisateur. Aucun droit pour les autres utilisateurs, à l'exception du répertoire pdf pour lesquels le droit d'écriture est accordé.
- Fichiers, propriété et droits:
 - Propriété de l'utilisateur système www-data, groupe www-data.
 - Droits de lecture, écriture pour l'utilisateur et le groupe utilisateur. Aucun droit pour les autres utilisateurs.

Comparaison serveurs web Apache / Nginx

	<u>Apache</u>	<u>Nginx</u>
Architecture de base	Processus/Thread	Evenements
Performance	Moyenne sous fort trafic	Bonne
Chargement dynamique des modules	Oui	Pas nativement
Traitement du contenu dynamique des pages	Oui	Pas nativement
Configuration décentralisée via fichier .htaccess	 Oui	Pas nativement

Serveur web configuration Apache:

extranet.rainbowbank.com

http port: 80

```
<VirtualHost 150.10.0.4:80>
    ServerName extranet.rainbowbank.com
    ServerAdmin admin@rainbowbank.com
    DocumentRoot /var/www/rainbowbank/extranet.rainbowbank.com/
    ErrorLog /var/www/rainbowbank/log/apache_error.log
    CustomLog /var/www/rainbowbank/log/apache_access_extranet.log combined
    Redirect permanent / https://extranet.rainbowbank.com/
</VirtualHost>
```

https port: 443

```
<VirtualHost 150.10.0.4:443>
    ServerName extranet.rainbowbank.com
    ServerAdmin admin@rainbowbank.com
    DocumentRoot /var/www/rainbowbank/extranet.rainbowbank.com/
    <Directory '/var/www/rainbowbank'>
        Options -Indexes +FollowSymLinks
    </Directory>
    ErrorLog /var/www/rainbowbank/log/apache_error.log
    CustomLog /var/www/rainbowbank/log/apache_access_extranet.log combined
    SSLEngine on
    SSLCertificateFile /var/www/rainbowbank/TLS_Certificat/self-signed/rainbowbank.com_SS.crt
    SSLCertificateKeyFile /var/www/rainbowbank/TLS_Certificat/self-signed/rainbowbank.com_SS.key
    Header always set Strict-Transport-Security "max-age=15768000"
</VirtualHost>
```

Écoute sur IP externe, port 80 (http) et 443 (https)
Nom du serveur: extranet.rainbowbank.com
Localisation des fichiers du site

Localisation des fichiers log d'erreur et de connexions

Redirection permanente des requêtes http vers https avec directive 'Redirect'

Désactive l'indexation de la structure du site

Activation du protocole SSL/TLS (https), avec localisation du certificat auto-signé et de la clés associé

Serveur web configuration Apache:

admin.rainbowbank.com

http port: 5501

```
<VirtualHost 192.168.10.5:5501>
  ServerName admin.rainbowbank.com
  ServerAdmin admin@rainbowbank.com
  DocumentRoot /var/www/rainbowbank/admin.rainbowbank.com/
  ErrorLog /var/www/rainbowbank/log/apache_error.log
  CustomLog /var/www/rainbowbank/log/apache_access_admin.log combined
  RewriteEngine On
  RewriteCond %{SERVER_PORT} 5501
  RewriteCond %{SERVER_NAME} =admin.rainbowbank.com
  RewriteRule ^ https:// %{SERVER_NAME}:5502%{REQUEST_URI} [END,NE,R=permanent]
</VirtualHost>
```

https port: 5502

```
<VirtualHost 192.168.10.5:5502>
  ServerName admin.rainbowbank.com
  ServerAdmin admin@rainbowbank.com
  DocumentRoot /var/www/rainbowbank/admin.rainbowbank.com/
  <Directory '/var/www/rainbowbank'>
    Options -Indexes +FollowSymLinks
  </Directory>
  ErrorLog /var/www/rainbowbank/log/apache_error.log
  CustomLog /var/www/rainbowbank/log/apache_access_admin.log combined
  SSLEngine on
  SSLCertificateFile /var/www/rainbowbank/TLS_Certificat/CA/rainbowbank.com_CA.crt
  SSLCertificateKeyFile /var/www/rainbowbank/TLS_Certificat/CA/rainbowbank.com_CA.key
  Header always set Strict-Transport-Security "max-age=15768000"
</VirtualHost>
```

Écoute sur IP interne, port 5501 (http) et 5502 (https)
Nom du serveur: admin.rainbowbank.com
Localisation des fichiers du site

Localisation des fichiers log d'erreur et de connexions

Redirection permanente des requêtes http vers https avec directive 'Rewrite', pour prendre en compte les ports non conventionnels.

Désactive l'indexation de la structure du site

Activation du protocole SSL/TLS (https), avec localisation du certificat et de la clé associée

Serveur web configuration Nginx:

extranet.rainbowbank.com

```
server {  
    listen 150.10.0.4:80;  
    server_name extranet.rainbowbank.com;  
    root /var/www/rainbowbank/extranet.rainbowbank.com;  
    index index.html;  
  
    error_log /var/www/rainbowbank/log/nginx_error.log;  
    access_log /var/www/rainbowbank/log/nginx_access_extranet.log;  
  
    return 301 https://$host$request_uri; } }
```

```
server {  
    listen 150.10.0.4:443 ssl;  
    server_name extranet.rainbowbank.com;  
    root /var/www/rainbowbank/extranet.rainbowbank.com;  
    index index.html;  
  
    error_log /var/www/rainbowbank/log/nginx_error.log;  
    access_log /var/www/rainbowbank/log/nginx_access_extranet.log;  
  
    ssl_certificate /var/www/rainbowbank/TLS_Certificat/self-signed/rainbowbank.com_SS.crt;  
    ssl_certificate_key /var/www/rainbowbank/TLS_Certificat/self-signed/rainbowbank.com_SS.key;  
  
    location / {  
        try_files $uri $uri/ =404;  
    } }
```

http port: 80

https port: 443

Écoute sur IP externe, port 80 (http) et 443 (https)
Nom du serveur: extranet.rainbowbank.com
Localisation des fichiers du site

Localisation des fichiers log d'erreur et de connexions

Redirection permanente des requêtes http vers https

Localisation du certificat auto-signé et de la clés associé

Serveur web configuration Nginx:

admin.rainbowbank.com

```
server {  
    listen 192.168.10.4:5501;  
    server_name extranet.rainbowbank.com;  
    root /var/www/rainbowbank/admin.rainbowbank.com;  
    index index.html;  
  
    error_log /var/www/rainbowbank/log/nginx_error.log;  
    access_log /var/www/rainbowbank/log/nginx_access_admin.log;  
  
    return 301 https://$host$request_uri;  
}
```

```
server {  
    listen 192.168.10.4:5502 ssl;  
    server_name extranet.rainbowbank.com;  
    root /var/www/rainbowbank/admin.rainbowbank.com;  
    index index.html;  
  
    error_log /var/www/rainbowbank/log/nginx_error.log;  
    access_log /var/www/rainbowbank/log/nginx_access_admin.log;  
  
    ssl_certificate /var/www/rainbowbank/TLS_Certificat/CA/rainbowbank.com_CA.crt;  
    ssl_certificate_key /var/www/rainbowbank/TLS_Certificat/CA/rainbowbank.com_CA.key;  
  
    location / {  
        try_files $uri $uri/ =404;  
    }  
}
```

http port: 5501

https port: 5502

Écoute sur IP interne, port 5501 (http) et 5502 (https)
Nom du serveur: admin.rainbowbank.com
Localisation des fichiers du site

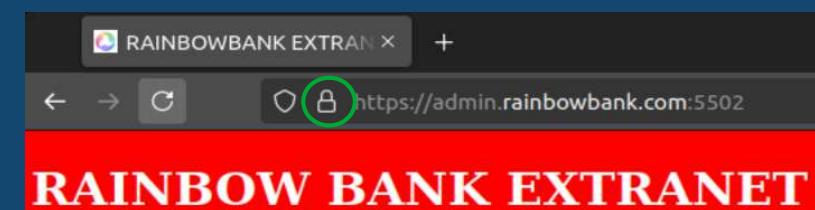
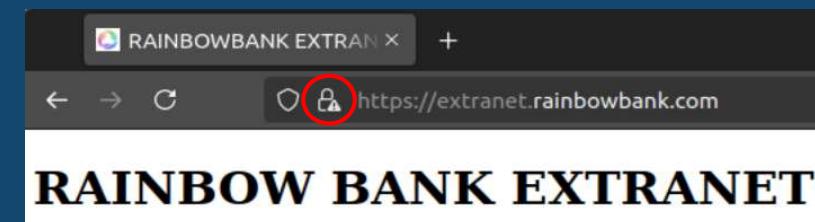
Localisation des fichiers log d'erreur et de connexions

Redirection permanente des requêtes http vers https

Localisation du certificat et de la clés associé

Configuration serveur web en https: protocole SSL/TLS

- SSL/TLS, permet l'authentification par certificat numérique du serveur, le chiffrement et l'intégrité des données échangées.
- Utilisation de l'outil OpenSSL pour générer les certificats.
- extranet.rainbowbank.com avec un certificat auto-signé:
 - Chiffrement et intégrité des données assuré
 - Authentification du serveur non-assuré avec message d'avertissement, car certificat non signé par une autorité de certification reconnue par le navigateur du client externe.
- admin.rainbowbank.com avec un certificat issu d'une ICP Rainbowbank:
 - L'ICP (Infrastructure à Clé Publique) permet en autre de créer une autorité de confiance pour le réseau interne Rainbowbank et d'émettre des certificats pour les sites qui seront reconnue sur le réseau interne.
 - Chiffrement et intégrité des données assuré
 - Authentification du serveur assuré sans message d'avertissement, car certificat reconnue par le navigateur du client, après diffusion du certificat de l'autorité de confiance sur les postes clients interne.



Configuration serveur web: certificats SSL/TLS

<https://extranet.rainbowbank.com>
Certificat auto-signé

Certificate	
*.rainbowbank.com	
Subject Name	
Country	FR
State/Province	ILE DE FRANCE
Locality	PARIS
Organization	RAINBOW BANK
Organizational Unit	DIRECTION INFRASTRUCTURE ET LOGISTIQUE
Common Name	*.rainbowbank.com
Email Address	admin@rainbowbank.com
Issuer Name	
Country	FR
State/Province	ILE DE FRANCE
Locality	PARIS
Organization	RAINBOW BANK
Organizational Unit	DIRECTION INFRASTRUCTURE ET LOGISTIQUE
Common Name	*.rainbowbank.com
Email Address	admin@rainbowbank.com
Validity	
Not Before	Wed, 22 May 2024 08:41:56 GMT
Not After	Thu, 22 May 2025 08:41:56 GMT

<https://admin.rainbowbank.com>
Certificat signé par autorité de certification interne

Certificate	
*.rainbowbank.com	
rainbowbank_root-ca	
Subject Name	
Country	FR
State/Province	ILE DE FRANCE
Locality	PARIS
Organization	RAINBOWBANK
Organizational Unit	DIRECTION INFRASTRUCTURE ET LOGISTIQUE
Common Name	*.rainbowbank.com
Email Address	admin@rainbowbank.com
Issuer Name	
Country	FR
State/Province	ILE DE FRANCE
Locality	PARIS
Organization	RAINBOWBANK
Organizational Unit	DIRECTION INFRASTRUCTURE ET LOGISTIQUE
Common Name	rainbowbank_root-ca
Email Address	admin@rainbowbank.com
Validity	
Not Before	Wed, 22 May 2024 15:53:26 GMT
Not After	Thu, 22 May 2025 15:53:26 GMT

Configuration serveur web: sécurité attaques

- Prévention attaque DDoS: module evasive
 - Déetecte un grand nombre de requête sur une courte période de temps, puis bloque les connections temporairement.

```
<IfModule mod_evasive20.c>
  DOSHashTableSize    3097
  DOSPageCount        5
  DOSPageInterval     1
  DOSSiteCount        50
  DOSSiteInterval      1
  DOSBlockingPeriod   10

  DOSEmailNotify      admin@rainbowbank.com
  DOSSystemCommand    "/bin/echo $(date)' - %s' >> /var/www/rainbowbank/log/apache_mod-evasive/evasive.log"
  DOSLogDir           "/var/www/rainbowbank/log/apache_mod-evasive"
  DOSWhiteList         127.0.0.1
</IfModule>
```

- Prévention attaque Slow connections: module ReqTimeout
 - Limite le temps maximum de maintient d'une connexion, puis déconnecte le client.

```
RequestReadTimeout header=20-40,minrate=500
RequestReadTimeout body=10,minrate=500
```

Protocole FTP, SFTP et FTPS comparaison:

Le protocole FTP (File Transfert Protocol) n'est pas sécurisé de base. Aucune authentification du serveur, ni de chiffrement des communications.

- FTPS (FTP via SSL/TLS):
 - Correspond à un FTP classique avec une surcouche SSL/TLS par dessus pour sécuriser l'ensemble.
 - Nécessite plusieurs port.
 - Nécessite un certificat SSL/TLS.
-
- SFTP (SSH FTP ou Secure File Transfert Protocol):
 - Correspond à une extension du protocole SSH permettant le transfert de fichiers.
 - Nécessite qu'un seul port pour fonctionner.

Service FTP configuration: ProFTPD

```
ServerName "Rainbow Bank Admin FTP"
Port 21
PassivePorts 50000 50100
}
RootLogin off
RequireValidShell off
AllowStoreRestart on
AllowRetrieveRestart on
MaxInstances 10
Umask 001 001
AccessGrantMsg "Rainbow Bank Admin FTP, %u connected"
DefaultRoot /var/www/rainbowbank/images-sites www-gra
DefaultRoot /var/www/rainbowbank
<Limit LOGIN>
    AllowGroup OR www-dev,www-gra
    DenyAll
</Limit>
<IfGroup OR www-dev www-gra>
    <Limit LOGIN>
        Allow 192.168.10.0/24
        DenyAll
    </Limit>
</IfGroup>
<IfModule mod_tls.c>
    TLSEngine on
    TLSLog /var/log/proftpd/tls.log
    TLSProtocol TLSv1.2
    TLSRSACertificateFile /etc/ssl/rainbowbank.com_SS.crt
    TLSRSACertificateKeyFile /etc/ssl/rainbowbank.com_SS.key
    TLSRequired off
</IfModule>
```

Création de deux groupes utilisateurs: www-dev et www-gra.

Pour utiliser le service FTP, l'utilisateur devra appartenir au groupe utilisateur www-dev ou www-gra, et aussi au groupe www-data.

Ports: 21 pour les connexions et entre 50000 – 50100 pour les données.

Accès autorisé uniquement pour les membres des groupes utilisateurs www-dev et www-gra.

Chroot (racine du système de fichier vu par l'utilisateur):

- Groupe www-dev: /var/www/rainbowbank
- Groupe www-gra: /var/www/rainbowbank/images-sites

Accès autorisé uniquement sur le réseau interne 192.168.10.0/24

Activation et configuration du protocole TLS pour passer en FTPS

Fail2ban configuration:

```
[INCLUDES]
before = paths-debian.conf

[DEFAULT]
ignoreip = 127.0.0.1/8 ::1
bantime = 5m
findtime = 5m
maxretry = 3
backend = auto
destemail = admin@rainbowbank.com
sender = extranet-fail2ban@rainbowbank.com

}

[sshd]
port      = ssh
logpath  = %(sshd_log)s
backend   = systemd

}

[apache-auth]
enabled = true
port     = http,https,5501,5502
logpath  = /var/www/rainbowbank/log/apache_*.log

}

[apache-status-code-custom]
enabled = true
filter   = apache-status-code-custom
port     = http,https,5501,5502
logpath  = /var/www/rainbowbank/log/apache_*.log
action   = iptables-allports[name=apache-status-code, protocol=tcp]

}

[proftpd]
enabled = true
port    = ftp,ftp-data,ftps,ftps-data
logpath = %(proftpd_log)s
```

{ Configuration générale Fail2ban

{ SSH: Surveillance des erreurs d'authentifications.

{ Apache: Surveillance des erreurs d'authentifications.

{ Apache: Surveillance des erreurs HTTP 403 (accès à la ressource interdit).

```
# Fail2Ban Apache status code 403 filter
# This filter is for access.log, NOT for error.log

[Definition]

failregex = ^<HOST> -.*"(GET|POST|HEAD).*HTTP.*" 403 \d+ ".*" ".*$"
ignoreregex =
datepattern = ^[^[]*\[(?P<DATE>[^]]*)\]
               {^LN-BEG}
```

{ ProFTPD: Surveillance des erreurs d'authentifications.

Netfilter configuration: filtrage IP

```
#!/bin/bash
# Script iptables rules, under /etc/network/if-up.d

# Flush iptables
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X
iptables -t raw -F
iptables -t raw -X

iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT

# Loopback (lo) traffic
iptables -A INPUT -i lo -j ACCEPT

# Maintain all established input connection
iptables -A INPUT -p tcp -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -p udp -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT } }

# ssh
iptables -A INPUT -i enp0s3 -p tcp --dport ssh -j ACCEPT }

# web extranet
iptables -A INPUT -i enp0s3 -p tcp -m multiport --dport 5501,5502 -j ACCEPT
iptables -A INPUT -i enp0s8 -p tcp -m multiport --dport http,https -j ACCEPT } }

# ftp: with ftp conntrack-helper activation for packets related to a ftp-session on default port.
iptables -t raw -A PREROUTING -p tcp --dport ftp -j CT --helper ftp -m comment --comment "ftp conntrack-helper activation"
iptables -A INPUT -i enp0s3 -p tcp --dport ftp -j ACCEPT -m comment --comment "ftp connection port"
# ftp-data port for active and passive mode covered by previous general rule maintain tcp RELATED,ESTABLISHED } }

# Deny all unless explicitly allowed
iptables -A INPUT -j DROP
iptables -A FORWARD -j DROP
```

Script bash de règles de filtrages iptables positionné sous /etc/network/if-up.d pour une exécution au démarrage système.

{ Accepte les connexions déjà établies ou en relations avec des connexions acceptées.

{ Accepte les connexions SSH sur le réseau interne (interface enp0s3).

{ Accepte les connexions sur les ports 5501 et 5502 (site admin) sur le réseau interne (interface enp0s3) et les ports 80 et 443 (site extranet) sur le réseau externe (interface enp0s8)

{ Accepte les connexions 'FTP connexion' et 'FTP donnée' induites.

Questions / Réponses

Voies d'améliorations :