GUIDE TECHNIQUE DÉTAILLÉ: SÉCURISATION WIFI AVEC FREERADIUS, LDAP ET PFSENSE

TABLE DES MATIÈRES

I. INSTALLATION DES PRÉREQUIS

1.1 Installation des paquets essentiels

```
# Mise à jour du système
apt update
apt upgrade -y

# Installation des outils de base
apt install -y nano net-tools iputils-ping wget curl
```

1.2 Configuration système

```
# Configuration du hostname
echo "radius-server" > /etc/hostname
hostname radius-server

# Ajouter dans /etc/hosts
echo "127.0.1.1 radius-server" >> /etc/hosts

# Redémarrage des services réseau
systemctl restart systemd-networkd
```

II. CONFIGURATION DE FREERADIUS

2.1 Installation de FreeRADIUS

```
# Installation des paquets FreeRADIUS
apt install -y freeradius freeradius-ldap freeradius-utils ssl-cert
```

```
# Vérification de l'installation
systemctl status freeradius
```

2.2 Configuration de base de FreeRADIUS

```
# Sauvegarde des fichiers originaux
cp /etc/freeradius/3.0/radiusd.conf /etc/freeradius/3.0/radiusd.conf.orig
cp /etc/freeradius/3.0/clients.conf /etc/freeradius/3.0/clients.conf.orig

# Configuration du fichier radiusd.conf
cat > /etc/freeradius/3.0/radiusd.conf << 'EOF'
prefix = /usr
exec_prefix = /usr
sysconfdir = /etc
localstatedir = /var
sbindir = ${exec_prefix}/sbin
logdir = /var/log/freeradius
raddbdir = /etc/freeradius/3.0
pidfile = ${run_dir}/radiusd.pid
user = freerad
group = freerad
max_request_time = 30
cleanup_delay = 5
max_requests = 16384
hostname_lookups = no
log {
    destination = files
    file = ${logdir}/radius.log
    syslog_facility = daemon
    stripped_names = yes
    auth = yes
    auth_badpass = yes
    auth_goodpass = yes
}
checkrad = ${sbindir}/checkrad
security {
    max_attributes = 200
    reject_delay = 1
    status_server = yes
}
proxy_requests = yes
thread pool {
    start_servers = 5
    max_servers = 32
    min_spare_servers = 3
    max_spare_servers = 10
    max_requests_per_server = 0
    auto_limit_acct = yes
}
EOF

# Redémarrage du service
systemctl restart freeradius
```

2.3 Configuration EAP

```
# Sauvegarde des fichiers originaux
cp /etc/freeradius/3.0/mods-available/eap /etc/freeradius/3.0/mods-available/eap.orig

# Génération des certificats
cd /etc/freeradius/3.0/certs/
./bootstrap

# Configuration du module EAP
```

```
cat > /etc/freeradius/3.0/mods-available/eap << 'EOF'
eap {
    default_eap_type = peap
    timer_expire = 60
    ignore_unknown_eap_types = no
    cisco_accounting_username_bug = no

    tls-config tls-common {
        private_key_password = whatever
        private_key_file = ${certdir}/server.key
        certificate_file = ${certdir}/server.pem
        ca_file = ${cadir}/ca.pem
        dh_file = ${certdir}/dh
        ca_path = ${cadir}
        cipher_list = "DEFAULT"
        cipher_server_preference = no
        tls_min_version = "1.2"
        tls_max_version = "1.2"
        ecdh_curve = "prime256v1"
    }

    tls {
        tls = tls-common
    }

    ttls {
        tls = tls-common
        default_eap_type = mschapv2
        copy_request_to_tunnel = yes
        use_tunneled_reply = yes
        virtual_server = "inner-tunnel"
    }

    peap {
        tls = tls-common
        default_eap_type = mschapv2
        copy_request_to_tunnel = yes
        use_tunneled_reply = yes
        virtual_server = "inner-tunnel"
    }

    mschapv2 {
    }
}
EOF

# Redémarrage du service
systemctl restart freeradius
```

2.4 Configuration des clients RADIUS

```
# Configuration des clients (points d'accès)
cat > /etc/freeradius/3.0/clients.conf << 'EOF'
client localhost {
    ipaddr = 127.0.0.1
    proto = *
    secret = testing123
    require_message_authenticator = no
    nas_type = other
}

client pfsense {
    ipaddr = 192.168.1.1
    secret = PfSenseRadiusSecret2024
    nas_type = other
    require_message_authenticator = yes
}
```

```
client ap_principal {
    ipaddr = 192.168.1.10
    secret = WifiApSecret2024
    nas_type = other
    require_message_authenticator = yes
}
EOF

# IMPORTANT: Remplacer les adresses IP et les secrets par les vôtres!

# Redémarrage du service
systemctl restart freeradius
```

III. CONFIGURATION DE LDAP

3.1 Installation de OpenLDAP

```
# Installation de OpenLDAP
apt install -y slapd ldap-utils

# Lors de l'installation, vous devrez définir un mot de passe admin

# Reconfiguration si nécessaire
dpkg-reconfigure slapd
# Répondez aux questions:
# - Omettre la configuration d'OpenLDAP? Non
# - Nom de domaine DNS: exemple.com
# - Nom d'organisation: Exemple
# - Mot de passe admin: VotreMotDePasse
# - Confirmer mot de passe: VotreMotDePasse
# - Moteur de base de données: MDB
# - Supprimer la base lors de la purge: Non
# - Déplacer ancienne base de données: Oui
```

3.2 Configuration de base LDAP

```
# Création d'un fichier LDIF pour la structure de base
cat > base.ldif << 'EOF'
dn: ou=users,dc=exemple,dc=com
objectClass: organizationalUnit
ou: users

dn: ou=groups,dc=exemple,dc=com
objectClass: organizationalUnit
ou: groups

dn: cn=wifi-users,ou=groups,dc=exemple,dc=com
objectClass: posixGroup
cn: wifi-users
gidNumber: 10000
EOF

# Ajouter la structure de base
ldapadd -x -D cn=admin,dc=exemple,dc=com -W -f base.ldif
# Entrez le mot de passe admin quand demandé
```

3.3 Ajout d'utilisateurs LDAP

```
# Création d'un fichier LDIF pour ajouter un utilisateur
cat > user1.ldif << 'EOF'
dn: uid=user1,ou=users,dc=exemple,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: user1
sn: Utilisateur
givenName: Premier
cn: Premier Utilisateur
displayName: Premier Utilisateur
uidNumber: 10000
gidNumber: 10000
userPassword: {SSHA}PasswordHashedValue
loginShell: /bin/bash
homeDirectory: /home/user1
EOF

# Générer un mot de passe hashé pour l'utilisateur
slappasswd -s MonMotDePasse
# Copiez la valeur {SSHA}... générée et remplacez {SSHA}PasswordHashedValue dans user1.ldif

# Ajouter l'utilisateur
ldapadd -x -D cn=admin,dc=exemple,dc=com -W -f user1.ldif
# Entrez le mot de passe admin quand demandé
```

IV. INTÉGRATION FREERADIUS-LDAP

4.1 Configuration du module LDAP dans FreeRADIUS

```
# Sauvegarde du fichier original
cp /etc/freeradius/3.0/mods-available/ldap /etc/freeradius/3.0/mods-available/ldap.orig

# Configuration du module LDAP
cat > /etc/freeradius/3.0/mods-available/ldap << 'EOF'
ldap {
    server = "localhost"
    port = 389
    identity = "cn=admin,dc=exemple,dc=com"
    password = VotreMotDePasseAdmin
    base_dn = "dc=exemple,dc=com"
    user {
        base_dn = "ou=users,${..base_dn}"
        filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
        scope = "sub"
    }
    group {
        base_dn = "ou=groups,${..base_dn}"
        filter = "(cn=%{Ldap-Group})"
        membership_attribute = "memberOf"
    }
    update {
        control:Password-With-Header    += 'userPassword'
        control:Ldap-UserDn             := 'dn'
        reply:Reply-Message             := 'radiusReplyMessage'
        reply:Tunnel-Type               := 'radiusTunnelType'
        reply:Tunnel-Medium-Type        := 'radiusTunnelMediumType'
        reply:Tunnel-Private-Group-ID   := 'radiusTunnelPrivateGroupId'
    }
    edir = no
    timeout = 4
    timelimit = 3
    net_timeout = 1
    start_tls = no
    pool {
```

```
        start = 5
        min = 4
        max = 10
        spare = 3
        uses = 0
        lifetime = 0
        idle_timeout = 60
    }
}
EOF

# Activer le module LDAP
ln -sf /etc/freeradius/3.0/mods-available/ldap /etc/freeradius/3.0/mods-enabled/

# Modification du fichier authorize pour utiliser LDAP
cp /etc/freeradius/3.0/sites-available/default /etc/freeradius/3.0/sites-available/default.orig
sed -i 's/-ldap/ldap/g' /etc/freeradius/3.0/sites-available/default

# Redémarrer FreeRADIUS
systemctl restart freeradius
```

4.2 Test de connexion

```
# Test avec un utilisateur LDAP
radtest user1 MonMotDePasse localhost 1812 testing123

# Si le test réussit, vous devriez voir "Access-Accept"
# Si le test échoue, vérifiez les logs:
tail -f /var/log/freeradius/radius.log
```

V. CONFIGURATION DE PFSENSE

5.1 Installation des packages

```
# Ces commandes doivent être exécutées dans la console pfSense (via SSH ou console)

# Installation des packages via pkg
pkg update
pkg install -y freeradius3 pfSense-pkg-LDAP
```

5.2 Configuration via l'interface web

```
# Accédez à l'interface web de pfSense et suivez ces étapes précises:

# 1. Configuration du service FreeRADIUS
# Allez à Services > FreeRADIUS
# Onglet Interfaces:
- Ajouter: Interface IP: LAN, Port: 1812, Type: Auth
- Ajouter: Interface IP: LAN, Port: 1813, Type: Acct

# 2. Configuration des clients RADIUS
# Allez à Services > FreeRADIUS > Clients
- Ajouter un client:
  Client Shortname: AP_Principal
  Client IP Address: 192.168.1.10
  Client Subnet: 32
  Client Secret: WifiApSecret2024
```

```
  Nastype: other
  Description: Point d'accès WiFi principal

# 3. Configuration du module LDAP
# Allez à Services > FreeRADIUS > LDAP
- Ajouter:
  Name: LDAP_Auth
  Hostname: 192.168.1.20
  Port: 389
  Base DN: dc=exemple,dc=com
  Filter: (uid=%{User-Name})
  Username Attribute: uid
  Password Attribute: userPassword
  Base Filter: (objectClass=posixAccount)
  Username: cn=admin,dc=exemple,dc=com
  Password: VotreMotDePasseAdmin
```

5.3 Configuration VLAN WiFi

```
# Configuration via interface web:

# 1. Création du VLAN
# Allez à Interfaces > Assignments > VLANs
- Ajouter:
  Parent interface: LAN
  VLAN Tag: 10
  Description: VLAN_WIFI

# 2. Assignation interface
# Allez à Interfaces > Assignments
- Ajouter (+): LAN_VLAN10
- Configurer:
  Enable: ✓
  Description: WIFI
  IPv4: Static
  IPv4 Address: 192.168.10.1/24

# 3. Configuration règles pare-feu
# Allez à Firewall > Rules > WIFI
- Ajouter:
  Action: Pass
  Interface: WIFI
  Protocol: Any
  Source: WIFI net
  Destination: Any
  Description: Allow WIFI to WAN
```

VI. CONFIGURATION DU POINT D'ACCÈS WIFI

6.1 Configuration WPA2-Enterprise

```
# Accédez à l'interface de votre point d'accès
# Ces paramètres sont génériques, adaptez-les à votre matériel spécifique:

# Pour un point d'accès Ubiquiti:
- SSID: Entreprise_Secure
```

```
- Security: WPA Enterprise
- Encryption: WPA2 AES/CCMP
- RADIUS Server: 192.168.1.1 (adresse IP pfSense)
- RADIUS Port: 1812
- RADIUS Secret: WifiApSecret2024
- RADIUS Accounting: Enabled
- RADIUS Accounting Port: 1813
- VLAN: 10

# Pour un point d'accès TP-Link:
- SSID: Entreprise_Secure
- Authentication Type: WPA/WPA2-Enterprise
- Encryption: AES
- RADIUS Server IP: 192.168.1.1
- RADIUS Port: 1812
- RADIUS Password: WifiApSecret2024
- Accounting RADIUS Server: Enabled
- Accounting RADIUS Port: 1813
- Accounting RADIUS Password: WifiApSecret2024
- VLAN ID: 10
```

VII. TEST ET DÉPANNAGE

7.1 Vérification des logs

```
# Sur le serveur FreeRADIUS:
tail -f /var/log/freeradius/radius.log

# Sur pfSense (via console ou SSH):
tail -f /var/log/system.log | grep -i radius

# Test avec radtest sur le serveur FreeRADIUS:
radtest user1 MonMotDePasse localhost 1812 testing123

# Test avec eapol_test (nécessite l'installation):
apt install -y libnl-3-dev libnl-genl-3-dev
git clone https://github.com/FreeRADIUS/freeradius-server.git
cd freeradius-server
./configure
cd scripts/travis
chmod +x eapol_test.sh
./eapol_test.sh
```

7.2 Commandes de dépannage

```
# Vérification de l'état du service FreeRADIUS
systemctl status freeradius

# Redémarrage du service FreeRADIUS
systemctl restart freeradius

# Test de la configuration OpenLDAP
ldapsearch -x -b "dc=exemple,dc=com" -H ldap://localhost

# Test utilisateur LDAP spécifique
ldapsearch -x -b "dc=exemple,dc=com" -H ldap://localhost "(uid=user1)"

# Vérification connectivité entre serveurs
ping 192.168.1.1
ping 192.168.1.10
```

```
ping 192.168.1.20

# Test ports ouverts
nc -zv 192.168.1.20 389
nc -zv 192.168.1.1 1812
nc -zv 192.168.1.1 1813

# Débogage des certificats
openssl verify -CAfile /etc/freeradius/3.0/certs/ca.pem /etc/freeradius/3.0/certs/server.pem

# Démarrage FreeRADIUS en mode debug
service freeradius stop
freeradius -X
```

7.3 Correctifs courants

```
# Problème: Erreur de connexion LDAP
# Solution: Vérifier les permissions
chown -R freerad:freerad /etc/freeradius/3.0/
chmod 640 /etc/freeradius/3.0/mods-enabled/ldap

# Problème: Certificats non reconnus
# Solution: Régénérer les certificats
cd /etc/freeradius/3.0/certs/
rm -f *.pem *.der *.csr *.crt *.key *.p12 serial* index.txt*
./bootstrap
chown -R freerad:freerad /etc/freeradius/3.0/certs/

# Problème: Impossible de se connecter au WiFi
# Solution: Vérifier les protocoles EAP
sed -i 's/default_eap_type = peap/default_eap_type = ttls/g' /etc/freeradius/3.0/mods-available/eap
systemctl restart freeradius

# Problème: Timeout dans les logs
# Solution: Augmenter les timeout
sed -i 's/timeout = 4/timeout = 10/g' /etc/freeradius/3.0/mods-enabled/ldap
sed -i 's/idle_timeout = 60/idle_timeout = 300/g' /etc/freeradius/3.0/mods-enabled/ldap
systemctl restart freeradius
```