FR

Guide Pratique

NAC avec OPNsense et FreeRADIUS

802.1X - Controle d acces reseau par VLAN dynamique

Mars 2026

Sommaire

1. Qu'est-ce que le NAC et pourquoi 802.1X ?
2. Prerequis
3. Installer le plugin FreeRADIUS sur OPNsense
4. Configurer FreeRADIUS : utilisateurs, certificats, EAP-TLS
5. Configurer les APs UniFi/Omada pour 802.1X
6. Configurer les switches (trunk + access 802.1X)
7. Tester : authentification reussie + rejet
8. Cas d'usage : BYOD, IoT, employes vs invites
9. Prochaines etapes : Suricata IDS/IPS

1. Qu'est-ce que le NAC et pourquoi 802.1X ?

Sur mon infra BOTUM, le firewall OPNsense segmente le reseau en VLANs. Mais la segmentation seule ne suffit pas -- n'importe quel appareil peut se connecter au WiFi ou brancher sur un port reseau et obtenir une IP dans le bon VLAN.

C'est la qu'intervient le **Network Access Control (NAC)** avec le protocole **802.1X** : chaque appareil doit s'authentifier avant d'obtenir l'acces reseau, et FreeRADIUS decide dans quel VLAN il est place.

802.1X est le standard IEEE qui permet cette authentification au niveau de la couche 2 (liaison de donnees). Le flux implique trois acteurs :

• **Supplicant** : l'appareil client (laptop, telephone, IoT) qui demande l'acces

• **Authenticator** : le switch ou AP WiFi qui relaie l'echange EAP vers le serveur RADIUS

• **Authentication Server** : FreeRADIUS sur OPNsense, qui accepte ou rejette la connexion

2. Prerequis

• OPNsense operationnel (voir Billet 1 : Installation dans Proxmox)

• VLANs configures (Employees, IoT, Guests) -- voir Billet 2 : VLANs Zero Trust

• APs UniFi ou Omada compatibles 802.1X -- voir Billet 4 : WiFi AP Management

• Switches manages avec support 802.1X (UniFi, TP-Link Omada, Cisco)

• Acces SSH admin a OPNsense

• Optionnel : autorite de certification (CA) interne pour EAP-TLS

3. Installer le plugin FreeRADIUS sur OPNsense

OPNsense propose le plugin os-freeradius via son gestionnaire de plugins. Ce plugin installe FreeRADIUS directement sur le routeur, sans serveur externe necessaire.

```
# OPNsense GUI :
# System -> Firmware -> Plugins
# Rechercher : freeradius
# Installer : os-freeradius (clic "+")

# Apres installation, recharger la page.
# Nouveau menu : Services -> FreeRADIUS

# Activer le service :
# Services -> FreeRADIUS -> General
# Enable FreeRADIUS : coche
# Interface : LAN
# Port RADIUS Auth : 1812
# Port RADIUS Acct : 1813
# Cliquer Save -> Apply
```

4. Configurer FreeRADIUS : utilisateurs, certificats, EAP-TLS

Creer les clients RADIUS (NAS)

Les clients RADIUS sont les switches et APs qui enverront les requetes d'authentification. Chaque client a un secret partage.

```
# Services -> FreeRADIUS -> Clients -> Add
# Name    : unifi-ap-01
# IP/CIDR : 192.168.X.X/32  (IP de l'AP ou switch)
# Secret  : [chaine aleatoire securisee]
# NAS Type: Other

# Repeter pour chaque AP et switch manage
```

Creer les utilisateurs et assigner les VLANs

Pour les authentifications PEAP-MSCHAPv2, creer des utilisateurs dans FreeRADIUS avec assignation VLAN dynamique :

```
# Services -> FreeRADIUS -> Users -> Add
# Username  : jean.dupont
# Password  : [mot de passe fort]
# VLAN ID   : 10  (VLAN Employes)

# Services -> FreeRADIUS -> Users -> Add
# Username  : device-iot-01
# Password  : [mot de passe fort]
# VLAN ID   : 30  (VLAN IoT)

# Le RADIUS envoie Tunnel-Private-Group-Id au switch/AP
# L'appareil est automatiquement place dans le bon VLAN
```

Configurer EAP-TLS avec certificats

EAP-TLS est la methode la plus securisee : l'authentification utilise des certificats X.509, sans mot de passe.

```
# 1. Creer une CA interne :
# System -> Cert. Manager -> Authorities -> Add
# Name         : BOTUM-Internal-CA
# Key Type     : RSA 4096
# Digest       : SHA256
# Lifetime     : 3650 jours

# 2. Creer le certificat serveur FreeRADIUS :
# System -> Cert. Manager -> Certificates -> Add
# Name         : freeradius-server-cert
# Authority    : BOTUM-Internal-CA
# Type         : Server Certificate

# 3. Configurer EAP dans FreeRADIUS :
# Services -> FreeRADIUS -> EAP
# Certificate  : freeradius-server-cert
# CA           : BOTUM-Internal-CA
# EAP Type     : TLS + PEAP
# Inner Method : MSCHAPv2 (pour PEAP sans certificat client)
```

5. Configurer les APs UniFi/Omada pour 802.1X

Dans UniFi Network Controller, configurer le reseau WiFi pour utiliser WPA-Enterprise (802.1X) au lieu de WPA-Personal :

```
# UniFi Controller -> Settings -> WiFi -> Add Network
# Name (SSID)    : BOTUM-Corp
# Security       : WPA Enterprise  (pas WPA Personal)
# RADIUS Profile : Creer nouveau

# RADIUS Profile :
# Auth Server IP   : [IP OPNsense LAN, ex. 192.168.1.1]
# Auth Server Port : 1812
# Auth Server Password : [secret configure dans FreeRADIUS]

# Le RADIUS renverra le VLAN via Tunnel-Private-Group-Id
# Appliquer sur les APs corporate (pas le WiFi invites)
```

6. Configurer les switches (trunk + access 802.1X)

Sur un switch manage, activer 802.1X par port pour les ports d'acces :

```
# UniFi Switch -- Port Profile avec 802.1X :
# Settings -> Profiles -> Switch Port Profiles -> Add
# 802.1X Control    : auto
# RADIUS Profile    : [profil RADIUS]
# VLAN par defaut   : VLAN 99 (quarantaine)
# VLAN post-auth    : Assigne par RADIUS dynamiquement

# Reference generique Cisco IOS :
# interface GigabitEthernet0/1
#  switchport mode access
#  switchport access vlan 99    <- VLAN quarantaine par defaut
#  dot1x pae authenticator
#  authentication port-control auto
#  authentication order dot1x mab
#  spanning-tree portfast
```

7. Tester : authentification reussie + rejet

Test avec radtest (CLI)

```
# Sur OPNsense (SSH ou System -> Shell) :
radtest jean.dupont [mot_de_passe] 127.0.0.1 0 [shared_secret]

# Resultat attendu (authentification reussie) :
# Sent Access-Request Id 1 from 127.0.0.1:xxxxx to 127.0.0.1:1812
# Received Access-Accept Id 1 from 127.0.0.1:1812
# Tunnel-Private-Group-Id = "10"   <- VLAN 10 assigne !
# Session-Timeout = 28800

# Test d'un device NON AUTORISE :
radtest intrus wrongpassword 127.0.0.1 0 [shared_secret]
# Resultat :
# Received Access-Reject Id 2 from 127.0.0.1:1812  -- bloque
```

Verification du placement VLAN

```
# Apres authentification reussie, verifier l'IP obtenue :
# Appareil employe  -> IP dans 192.168.10.x  (VLAN 10 OK)
# Appareil IoT      -> IP dans 192.168.30.x  (VLAN 30 OK)
# Appareil inconnu  -> IP dans 192.168.99.x  (VLAN 99 quarantaine)
#                      ou rejete completement

# Logs FreeRADIUS en temps reel :
# Services -> FreeRADIUS -> Log File
# Filtrer Accept/Reject pour audit complet
```

8. Cas d'usage : BYOD, IoT, employes vs invites

• **Employes (VLAN 10)** : laptops corporate avec certificat EAP-TLS ou compte PEAP -> acces reseau interne complet

• **BYOD -- Bring Your Own Device (VLAN 20)** : appareils personnels avec compte PEAP -> acces internet uniquement

• **IoT (VLAN 30)** : cameras, capteurs, imprimantes via MAC Authentication Bypass (MAB) -> isoles dans leur VLAN

• **Invites (VLAN 99)** : portail captif ou SSID separe sans 802.1X -> acces internet filtre

• **Appareils inconnus** : rejet total ou VLAN quarantaine selon la politique de securite

9. Prochaines etapes : Suricata IDS/IPS

Le Billet 7 couvrira **Suricata IDS/IPS** sur OPNsense : detection d'intrusion en temps reel, regles Emerging Threats, et integration CrowdSec pour une protection en profondeur.

Combine avec le NAC 802.1X de ce billet, vous aurez une stack de securite complete et Enterprise-grade.

Article complet : blog.botum.ca/opnsense-nac-freeradius-802-1x

Site web : www.botum.ca • contact@botum.ca