

---

# Réseau et Sécurité

Par Clément Lardeux, Clément Nonnotte, Béranger Lamarche et Robin Minaud

---

# Architecture

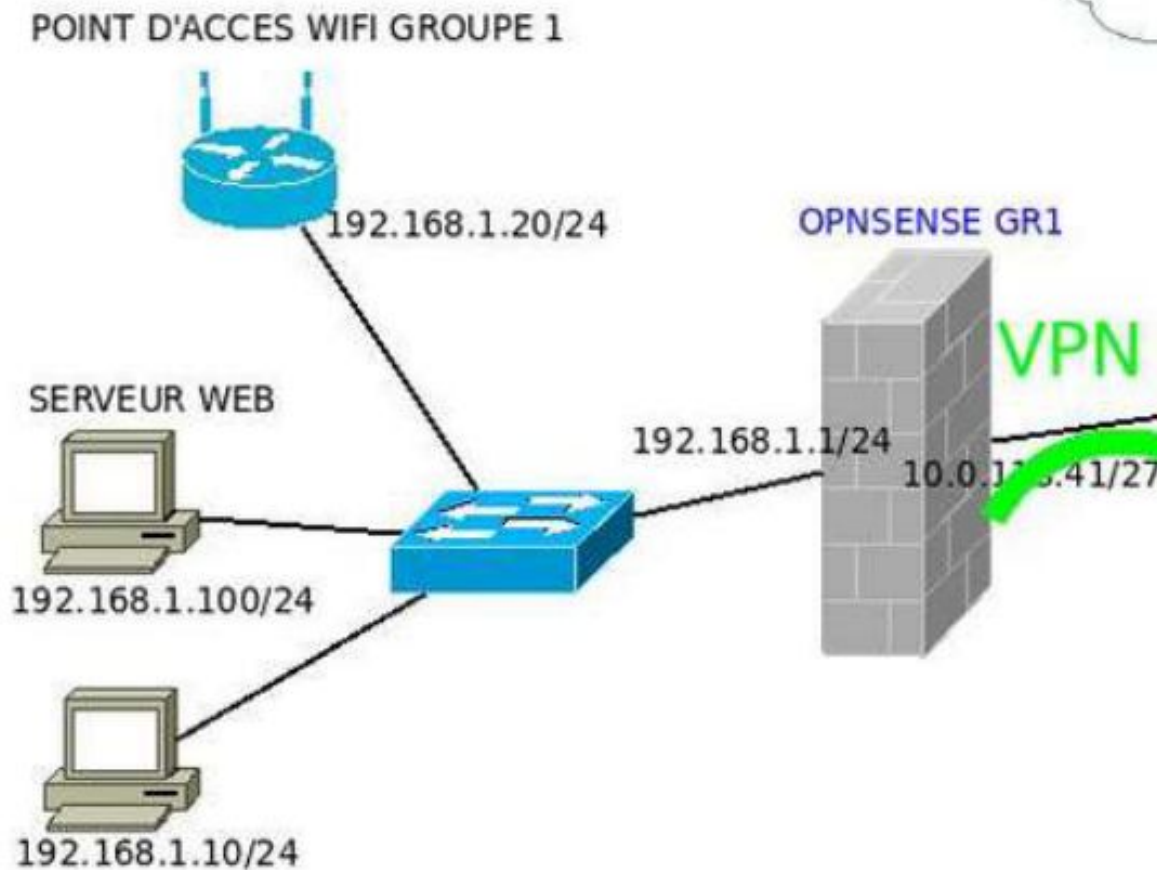
Point d'accès : 192.168.1.20

Firewall : 192.168.1.1

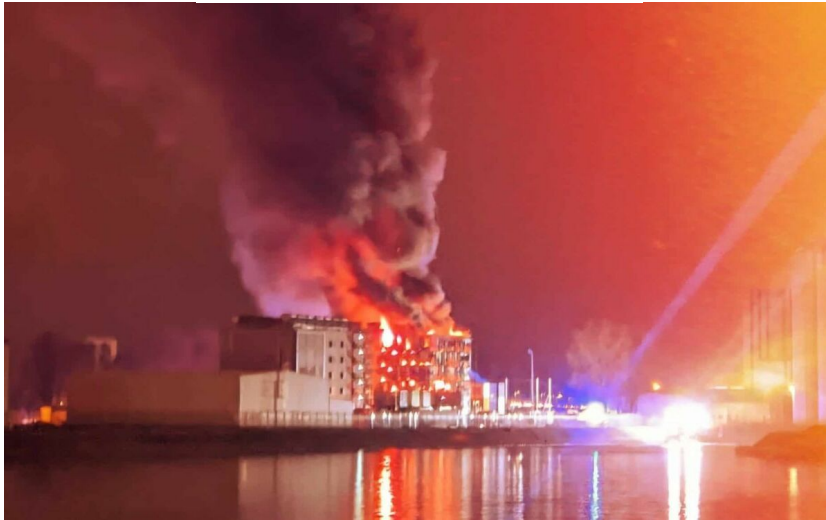
Serveur WEB : 192.168.1.100

PC utilisateur : 192.168.1.10

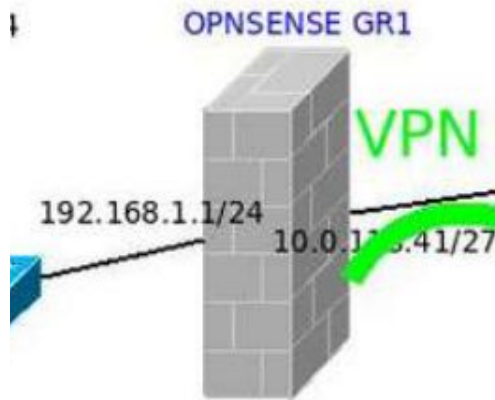
VPN :



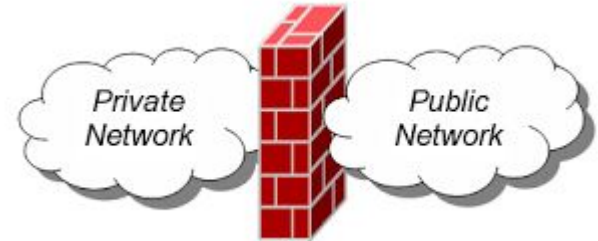
# Serveur Web



# Firewall



re1 : LAN ip : 192.168.1.1/24  
re1 : WAN ip : 10.0.118.41/27



Règles du firewall :

✗	IPv4 UDP	This Firewall	*	*	*
✗	IPv4 TCP	This Firewall	80 (HTTP)	*	80 (HTTP)

# Bilan sécurité

Point d'accès : Clé WPA "azerty123456789"

Firewall :

- Blocages protocole UDP
- Blocages HTTP sous protocole TCP
- Redirection des requêtes SSH

VPN : Pre-shared key "jesusleking"



# Bilan gestion de communication

Répartition des différentes tâches

Résolution des problèmes



# Attaque



# Conclusion

