

Projet 1 - Modernisation et sécurisation du site principal

Scénario 1 : Sécurisation réseau et segmentation VLAN

Nom / Prénom	Samy DESMAZEAUX
Formation	BTS SIO - Option SISR
Session	2026
Entreprise support	EcoSolar Solutions
Version du document	V1 - éléments réalisés + captures fournies
Date	02/06/2026

Périmètre V1 : éléments prouvés par captures - topologie GNS3, VLAN, trunk, interfaces pfSense, DHCP, règles firewall de test et validations de connectivité.

Sommaire

1. Analyse du besoin

2. Conditions de réalisation

3. Conception de la solution

4. Mise en œuvre technique réalisée

5. Tests et validation

6. Synthèse des résultats obtenus

7. Compétences du référentiel mobilisées

8. Conclusion

9. Annexes - preuves et correspondance des captures

1. Analyse du besoin

1.1 Contexte général

EcoSolar Solutions est une entreprise fictive spécialisée dans le développement et la fabrication de panneaux solaires à haut rendement. Son activité repose sur des données métiers sensibles : informations clients, documents commerciaux, gestion ERP/CRM, données liées à la production et éléments de conception protégés.

Le système d'information existant était initialement construit autour d'un réseau unique. Cette organisation simplifie l'administration au départ, mais elle devient risquée lorsque l'entreprise grandit : les postes utilisateurs, les serveurs, l'administration et les ressources exposées se retrouvent dans un même périmètre réseau.

L'objectif du scénario 1 est donc de poser une base réseau plus propre : séparer les usages par VLAN, centraliser le routage sur pfSense et préparer un filtrage plus précis des flux.

1.2 Contexte technique initial

- Réseau initial unique en 192.168.128.0/24, sans segmentation VLAN.
- Switch Cisco administrable utilisé comme cœur de réseau.
- Firewall pfSense placé en sortie du réseau.
- Absence de séparation claire entre les postes utilisateurs, les serveurs de production, les accès d'administration et la DMZ.
- Règles firewall initiales très permissives, insuffisantes pour une segmentation de sécurité.

1.3 Besoin principal

Le besoin principal est de segmenter le réseau local d'EcoSolar Solutions afin de limiter les communications inutiles entre les zones du SI et de créer une base plus sécurisée pour les services internes.

- Isoler les postes d'administration dans un VLAN dédié.
- Séparer les ressources de production des postes utilisateurs.
- Créer une zone DMZ pour les services exposés ou semi-exposés.
- Mettre en place le routage inter-VLAN via pfSense.
- Préparer des règles firewall adaptées à chaque zone.

2. Conditions de réalisation

2.1 Environnement de travail

- Travail réalisé dans un contexte pédagogique BTS SIO SISR.
- Maquette réalisée sur GNS3 avec pfSense, un switch Cisco / switch core, un NAT Internet et des hôtes VPCS.
- Administration du switch par console Solar-PuTTY.
- Administration de pfSense depuis l'interface web via Firefox.
- Documentation construite à partir des captures fournies et du contexte projet EcoSolar Solutions.

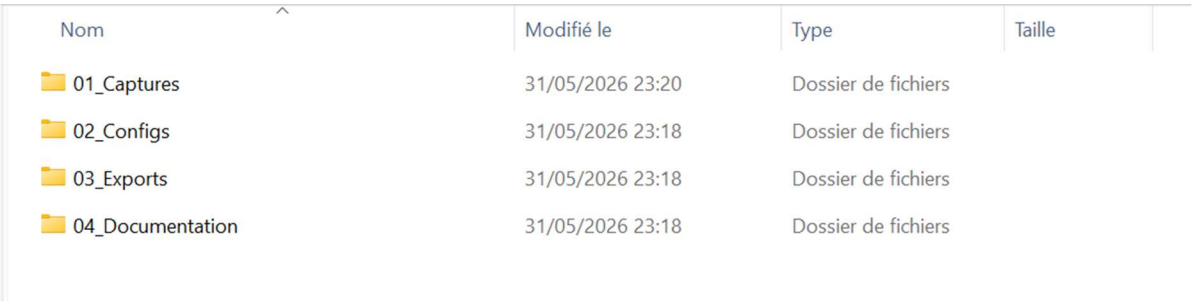


Figure 1 - Arborescence du dossier projet et préparation des preuves

3. Conception de la solution

3.1 Architecture cible retenue

La solution mise en place repose sur une architecture simple et lisible : le switch core transporte les VLAN jusqu'au firewall pfSense par un lien trunk 802.1Q. Les hôtes sont raccordés sur des ports access affectés à leur VLAN. pfSense porte les passerelles de chaque réseau et assure le routage entre les VLAN.

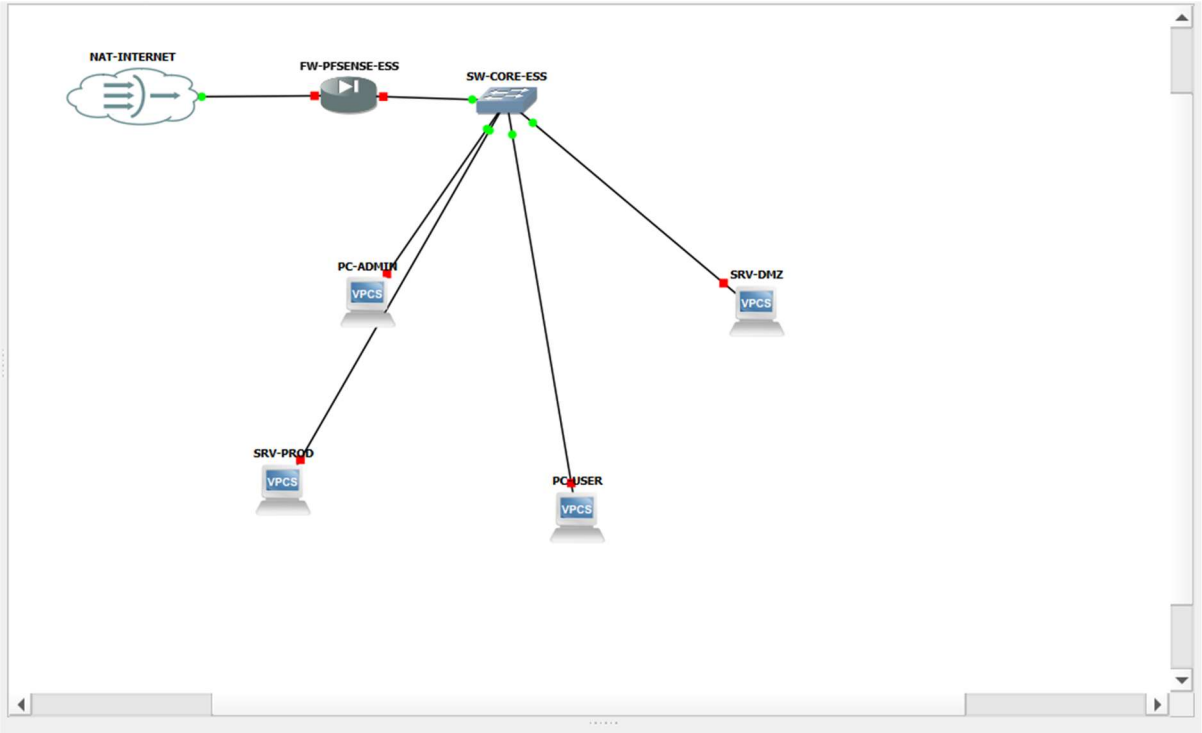


Figure 2 - Topologie GNS3 de la maquette VLAN EcoSolar Solutions

VLAN	Nom	Rôle	Réseau	Passerelle pfSense	Hôte de test
10	ADMIN	Administration	192.168.10.0/24	192.168.10.254	PC-ADMIN
20	PRODUCTION	Serveurs / production	192.168.20.0/24	192.168.20.254	SRV-PROD
30	USERS	Utilisateurs	192.168.30.0/24	192.168.30.254	PC-USER
40	DMZ	Zone DMZ	192.168.40.0/24	192.168.40.254	SRV-DMZ

VLAN	Nom	Rôle	Réseau	Passerelle pfSense	Hôte de test
99	NATIVE_PARKING	VLAN natif non utilisé	Non adressé dans la maquette	-	-

4. Mise en œuvre technique réalisée

4.1 Préparation des ports du switch dans GNS3

La topologie GNS3 utilise un switch central nommé SW-CORE-ESS. Les ports sont organisés avec un port trunk vers pfSense et des ports access vers les différents hôtes de test.

Port GNS3	Mode	VLAN	Usage
0	dot1q	Trunk	Lien vers pfSense
1	access	10	PC-ADMIN
2	access	20	SRV-PROD
3	access	30	PC-USER
4	access	40	SRV-DMZ

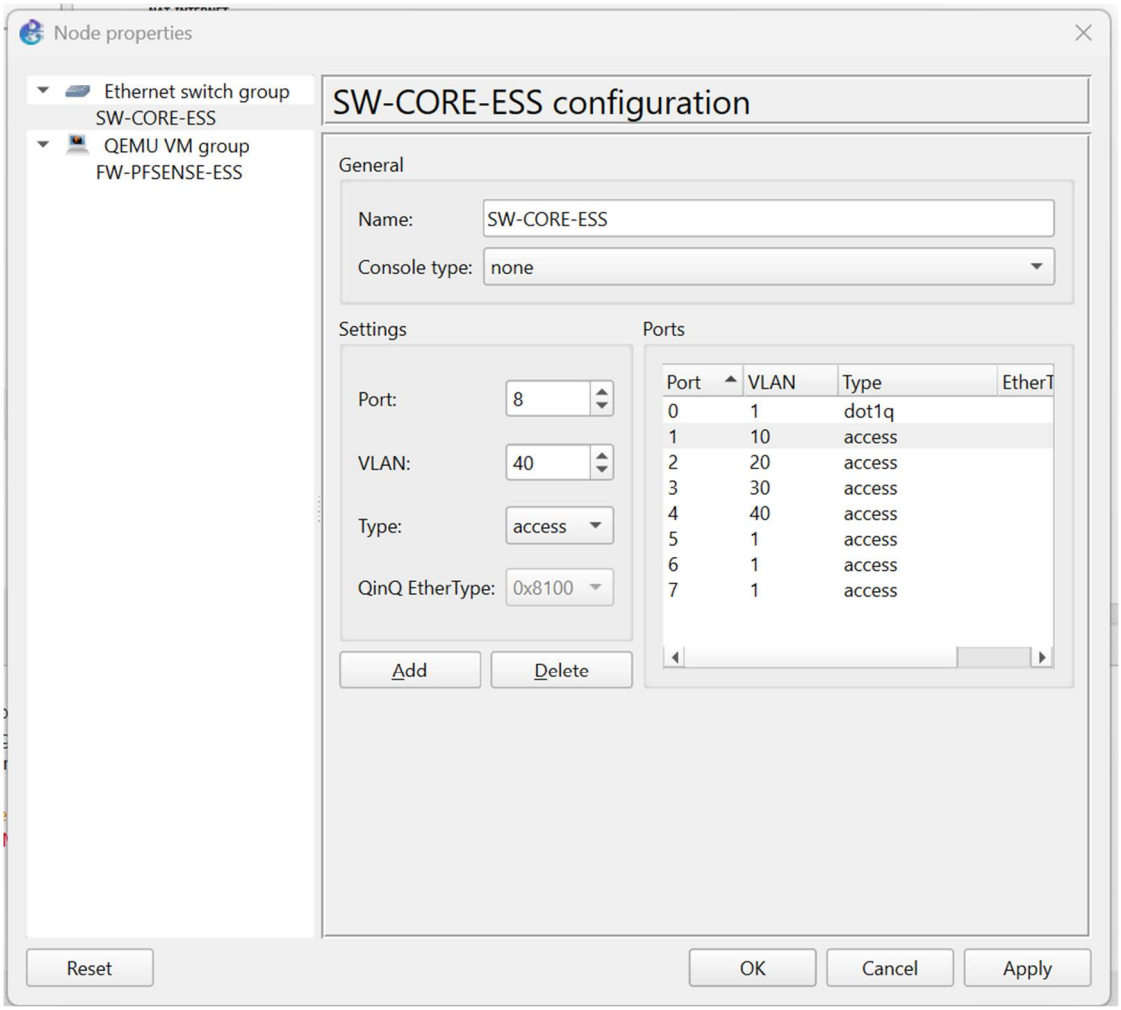


Figure 3 - Configuration des ports VLAN dans le switch GNS3

4.2 Configuration VLAN et trunk sur le switch Cisco

La configuration Cisco vérifie la création des VLAN et la mise en place du trunk 802.1Q. Le VLAN natif utilisé est le VLAN 99, nommé NATIVE_PARKING, ce qui évite d'utiliser le VLAN 1 comme VLAN natif opérationnel.

Élément configuré	Résultat observé
VLAN 10	ADMIN actif sur Et0/1
VLAN 20	PRODUCTION actif sur Et0/2
VLAN 30	USERS actif sur Et0/3
VLAN 40	DMZ actif sur Et1/0
Trunk Et0/0	Encapsulation 802.1Q, VLAN natif 99, VLAN autorisés 10, 20, 30, 40

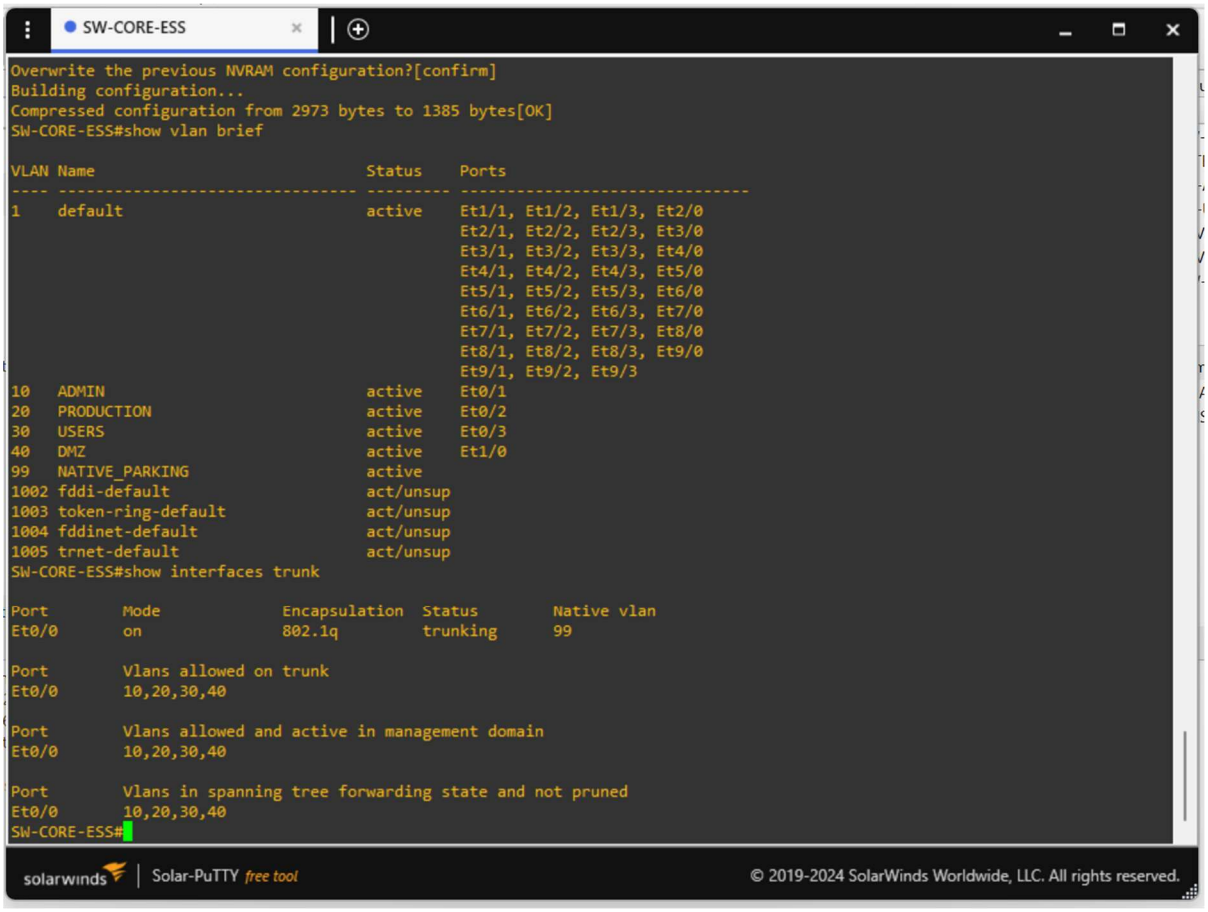


Figure 4 - Vérification Cisco : show vlan brief et show interfaces trunk

4.3 Création des VLAN sur pfSense

Les VLAN ont été créés sur l'interface LAN physique em1 de pfSense. Chaque VLAN correspond à un réseau logique distinct et à une future interface firewall dédiée.

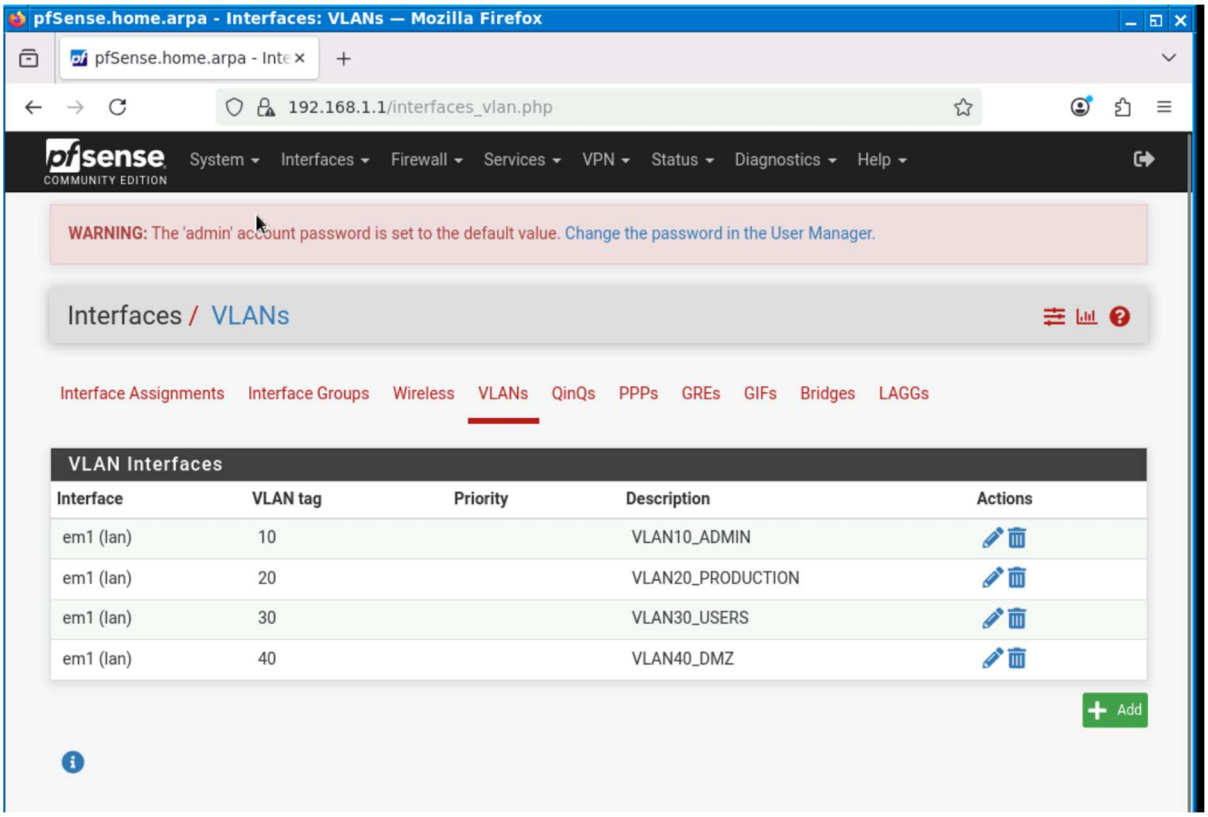


Figure 5 - Création des VLAN 10, 20, 30 et 40 dans pfSense

4.4 Assignation des interfaces pfSense

Après la création des VLAN, chaque interface virtuelle a été assignée dans pfSense. Les interfaces ADMIN, PRODUCTION, USERS et DMZ apparaissent désormais comme des interfaces firewall séparées.

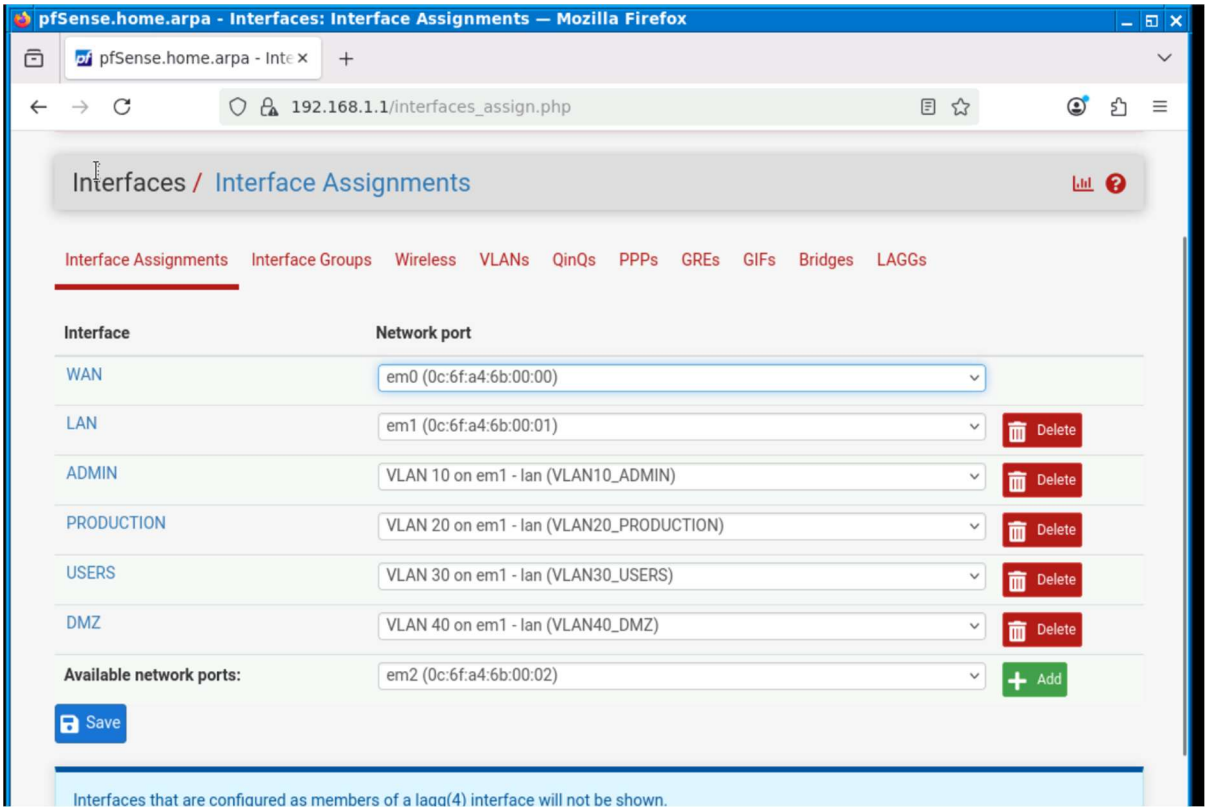


Figure 6 - Assignation des VLAN en interfaces pfSense

4.5 Configuration IPv4 des passerelles VLAN

Chaque interface VLAN pfSense reçoit une adresse IPv4 statique en .254. Cette adresse sert de passerelle par défaut pour les hôtes du VLAN concerné.

Interface pfSense	VLAN	Adresse passerelle
ADMIN	10	192.168.10.254/24
PRODUCTION	20	192.168.20.254/24
USERS	30	192.168.30.254/24
DMZ	40	192.168.40.254/24

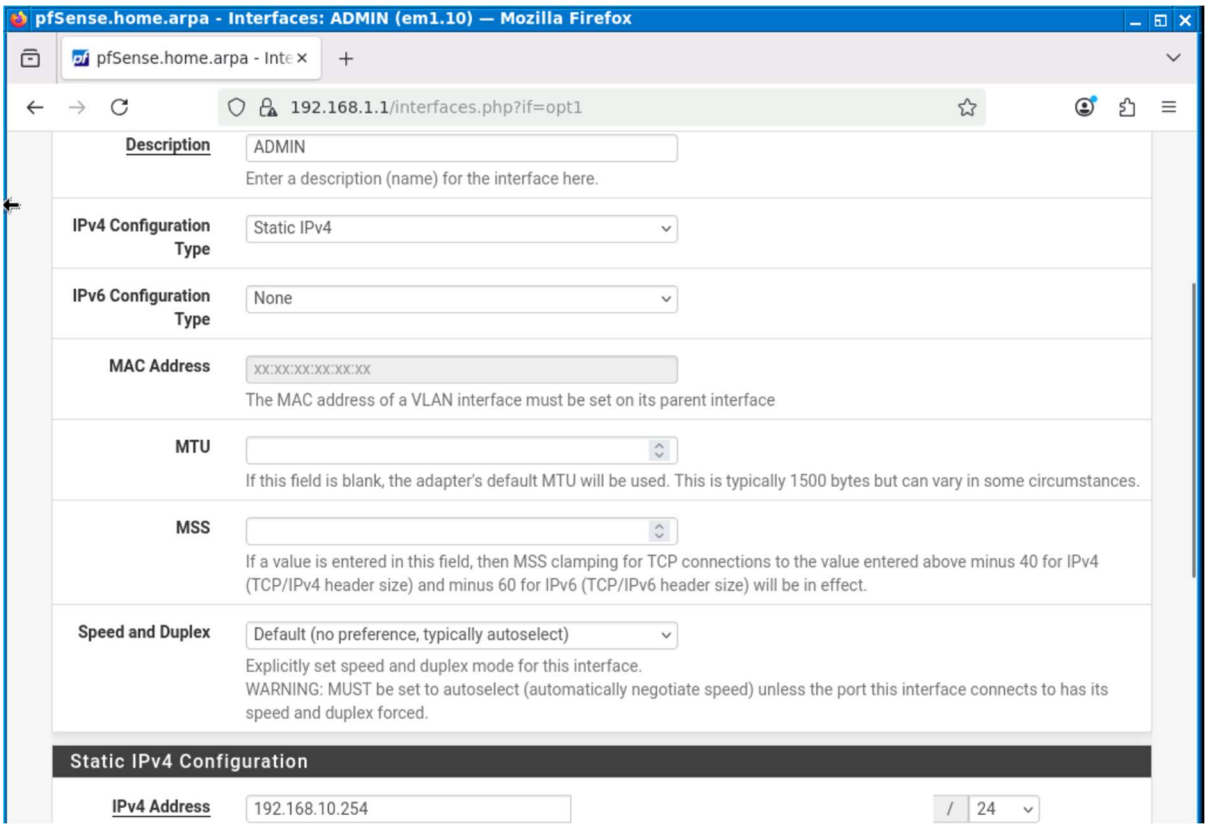


Figure 7 - Exemple de configuration IPv4 statique sur l'interface ADMIN

4.6 Activation du DHCP par VLAN

Le service DHCP de pfSense est activé sur les interfaces VLAN afin de distribuer automatiquement une adresse IP, une passerelle et un DNS aux hôtes de test. La capture ci-dessous illustre la configuration du DHCP sur le VLAN ADMIN avec une plage d'adresses allant de 192.168.10.10 à 192.168.10.100.

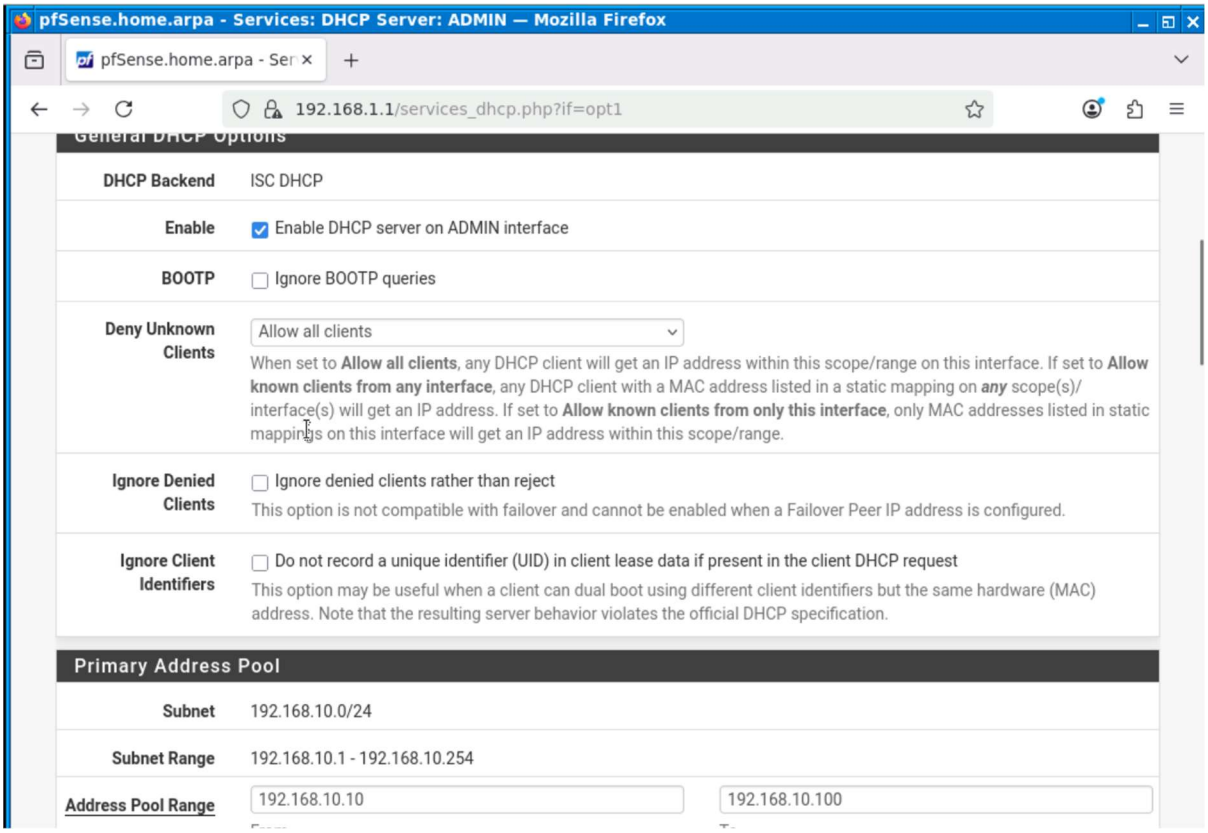


Figure 8 - Activation du DHCP sur le VLAN ADMIN

4.7 Règles firewall de validation

Pour valider rapidement la maquette, des règles temporaires de type Pass ont été appliquées sur les interfaces VLAN. Elles autorisent les flux IPv4 depuis le sous-réseau de l'interface vers n'importe quelle destination. Cette configuration sert à prouver le fonctionnement du routage et du DHCP avant un durcissement plus strict.

Paramètre	Valeur appliquée pour les tests
Action	Pass
Address Family	IPv4
Protocol	Any
Source	Sous-réseau de l'interface concernée
Destination	Any

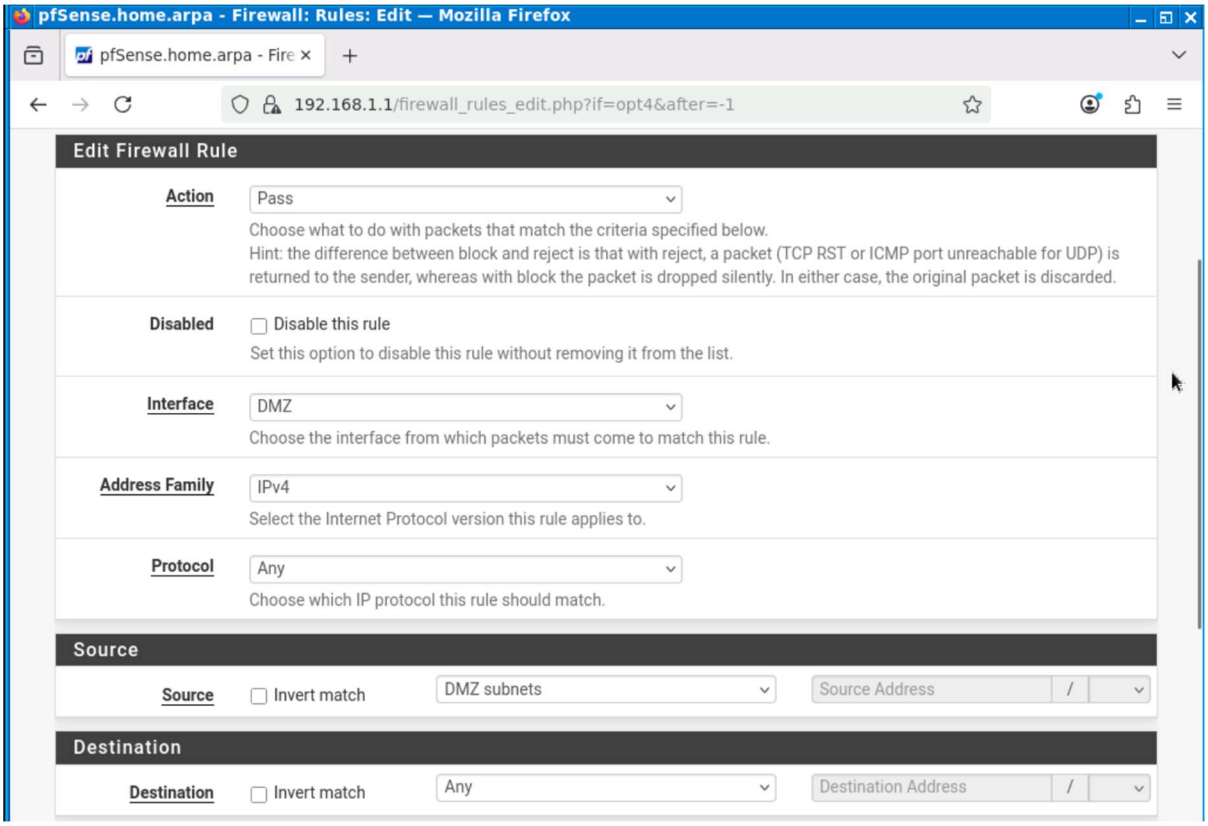


Figure 9 - Exemple de règle firewall temporaire sur l'interface DMZ

5. Tests et validation

5.1 Validation DHCP

Le premier contrôle consiste à vérifier que chaque machine reçoit une adresse IP dans le bon réseau. Les commandes dhcp puis show ip ont été lancées sur les hôtes VPCS.

Hôte	VLAN	Adresse reçue	Passerelle	Résultat
PC-ADMIN	10	192.168.10.10/24	192.168.10.254	Validé
SRV-PROD	20	192.168.20.10/24	192.168.20.254	Validé
PC-USER	30	192.168.30.10/24	192.168.30.254	Validé
SRV-DMZ	40	192.168.40.10/24	192.168.40.254	Validé

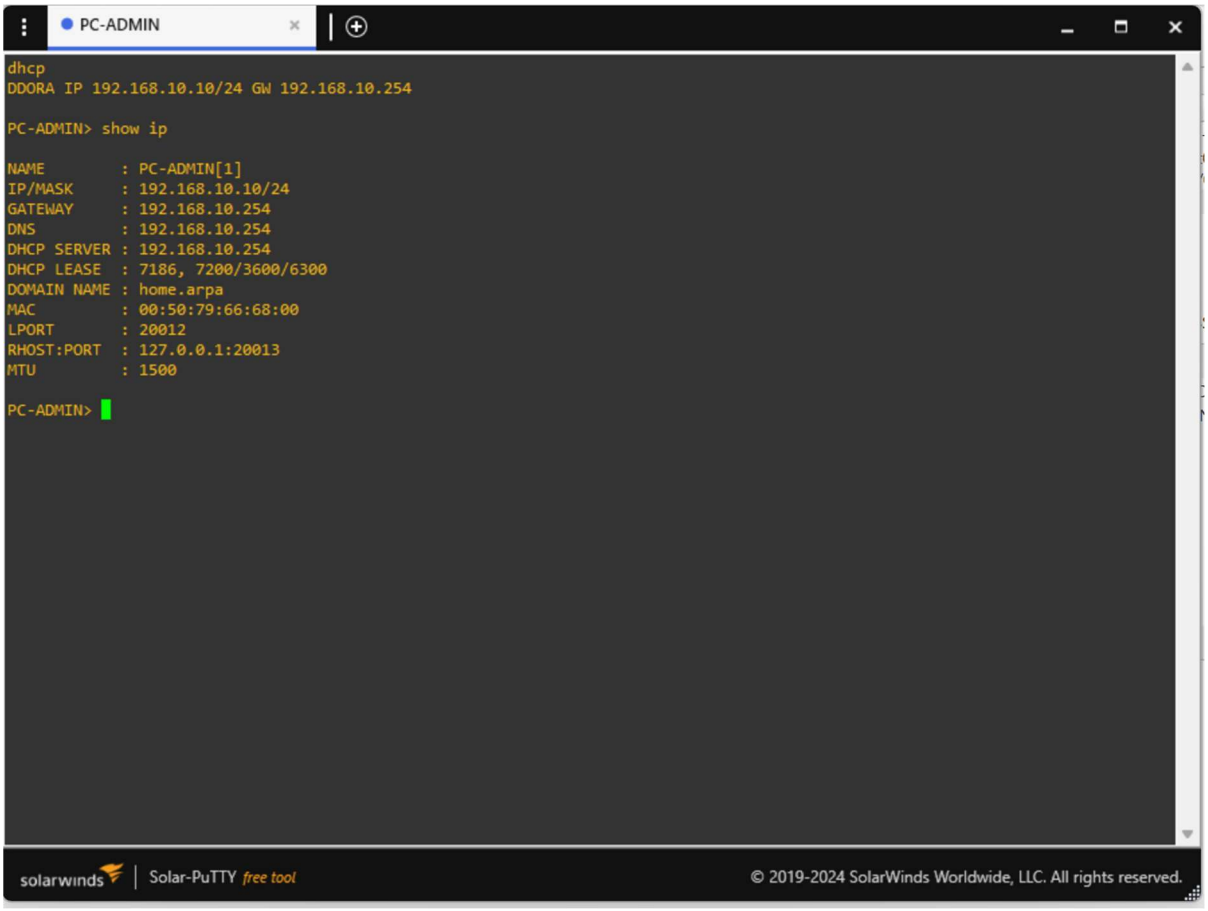


Figure 10 - Validation DHCP sur PC-ADMIN

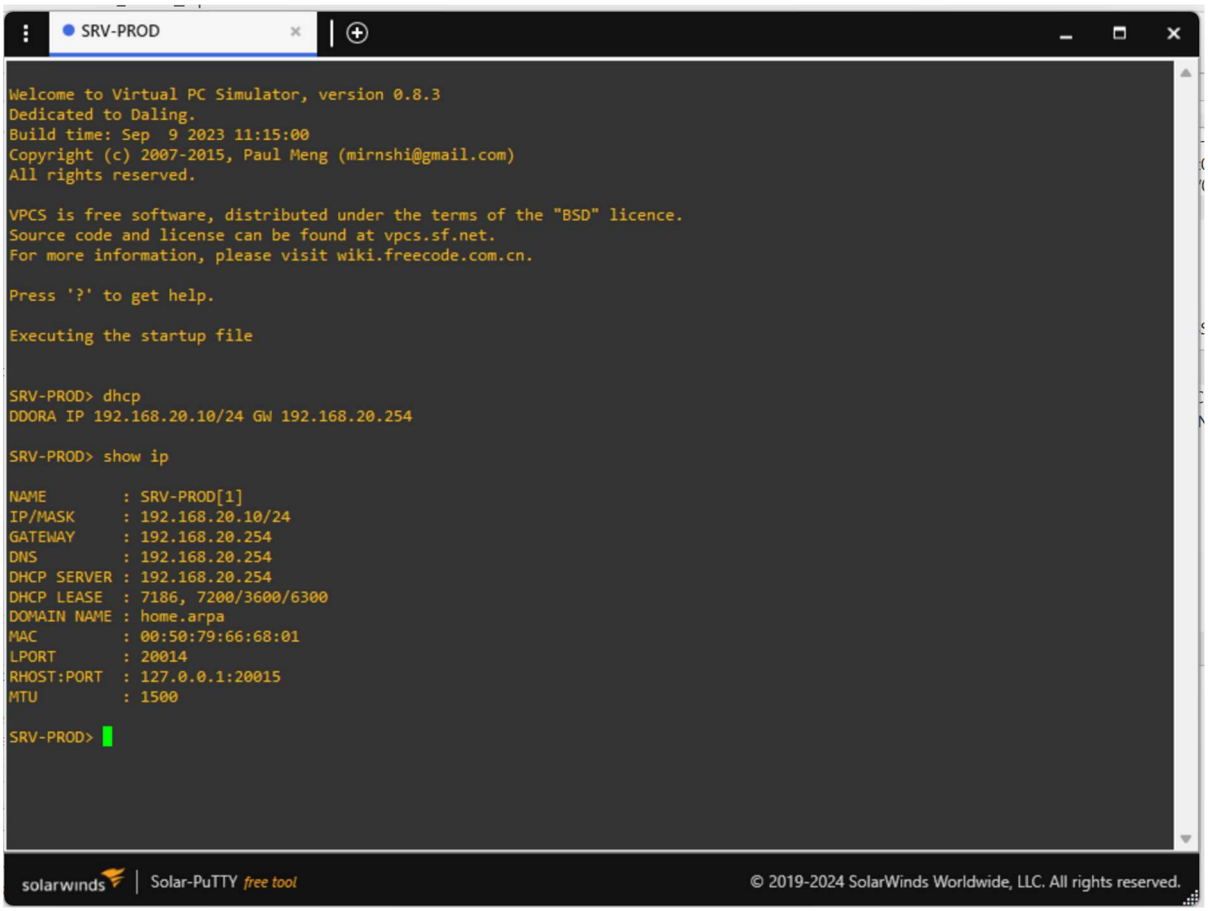


Figure 11 - Validation DHCP sur SRV-PROD



Figure 12 - Validation DHCP sur PC-USER

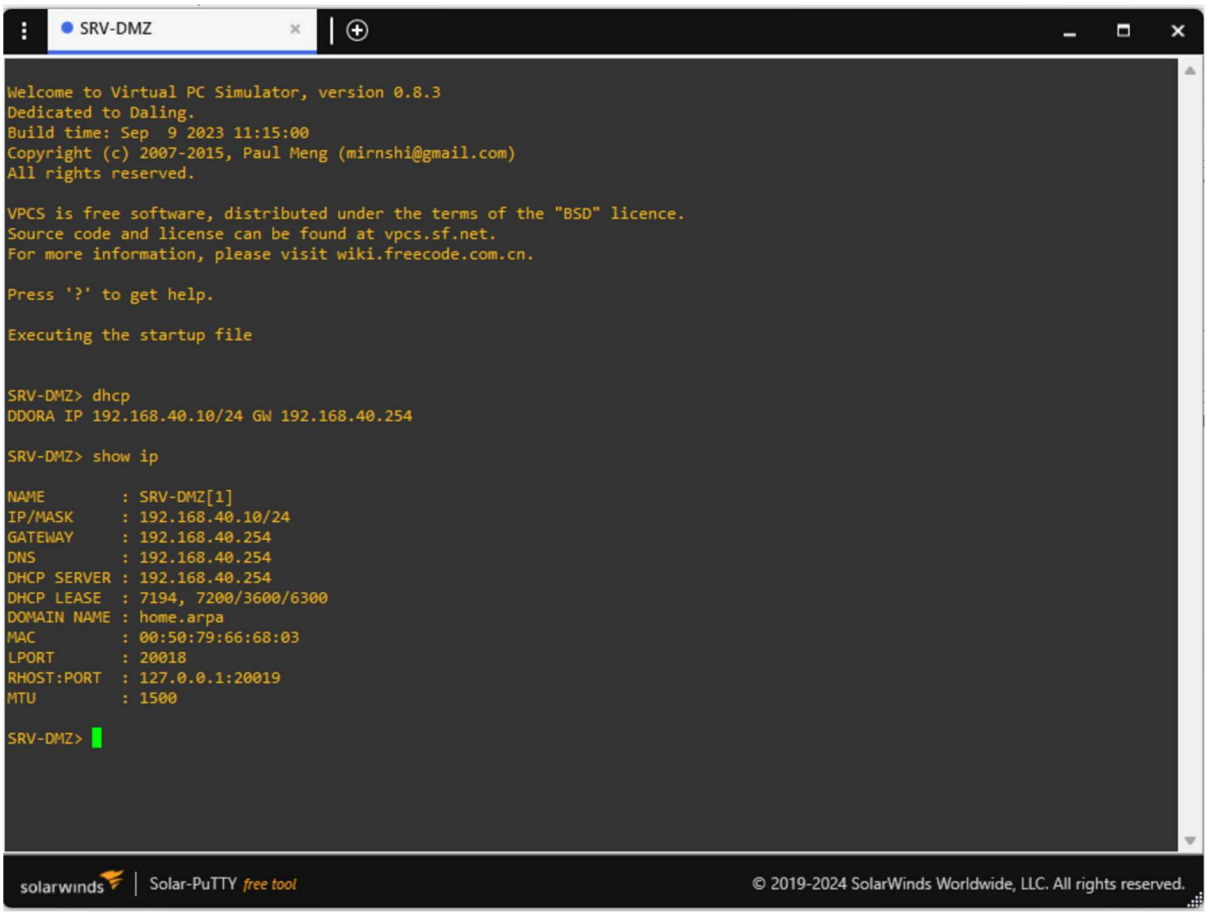


Figure 13 - Validation DHCP sur SRV-DMZ

5.2 Validation de la connectivité vers les passerelles VLAN

Les tests ICMP confirment que les hôtes peuvent joindre les passerelles pfSense des différents VLAN. Les réponses reçues montrent que les VLAN, le trunk et les interfaces pfSense sont cohérents.

Source de test	Destination testée	Observation
PC-ADMIN	192.168.10.254	Réponses ICMP reçues
PC-ADMIN	192.168.20.254	Réponses ICMP reçues
PC-ADMIN	192.168.30.254	Réponses ICMP reçues
PC-ADMIN	192.168.40.254	Réponses ICMP reçues
PC-USER	192.168.30.254	Réponses ICMP reçues
PC-USER	192.168.10.254	Réponses ICMP reçues
PC-USER	192.168.20.254	Réponses ICMP reçues
PC-USER	192.168.40.254	Réponses ICMP reçues

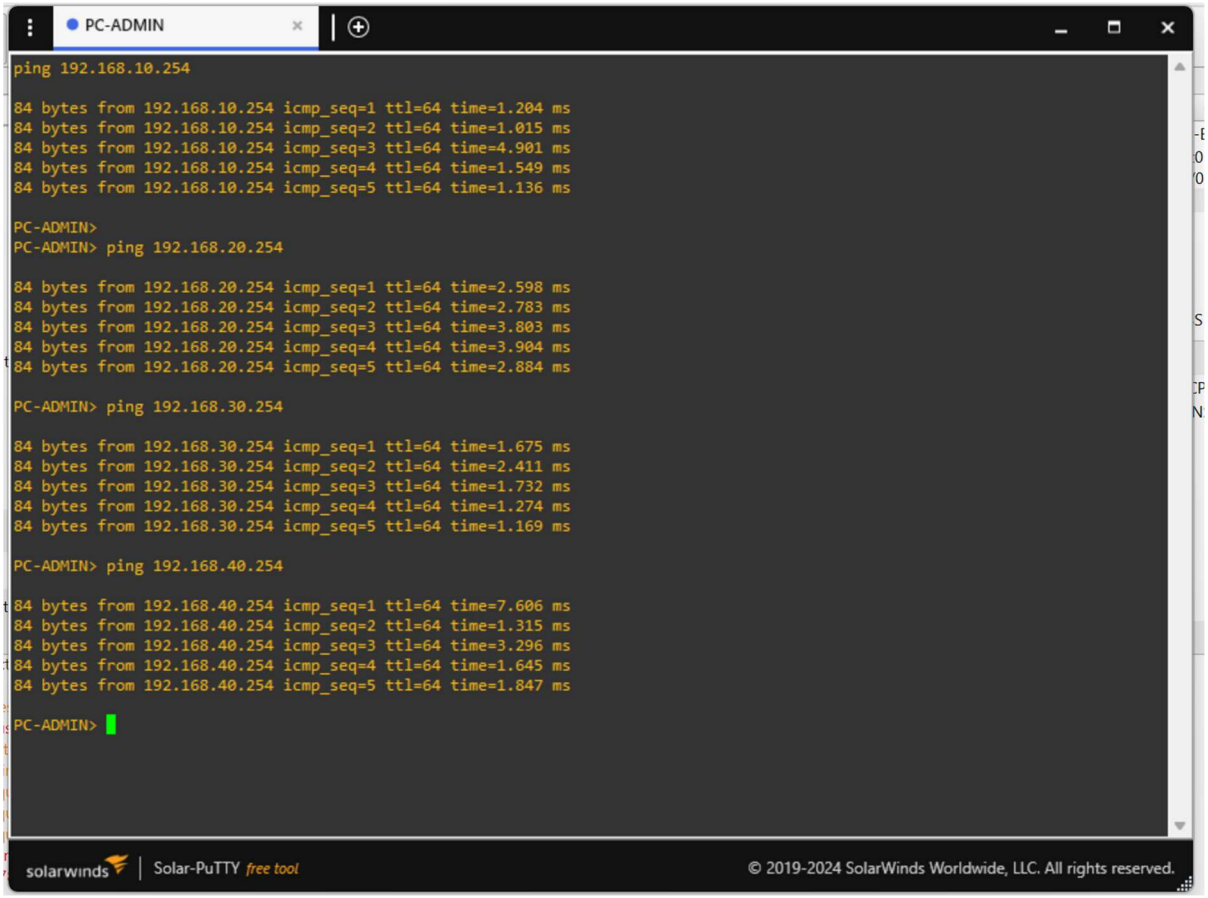


Figure 14 - Tests ping depuis PC-ADMIN vers les passerelles VLAN

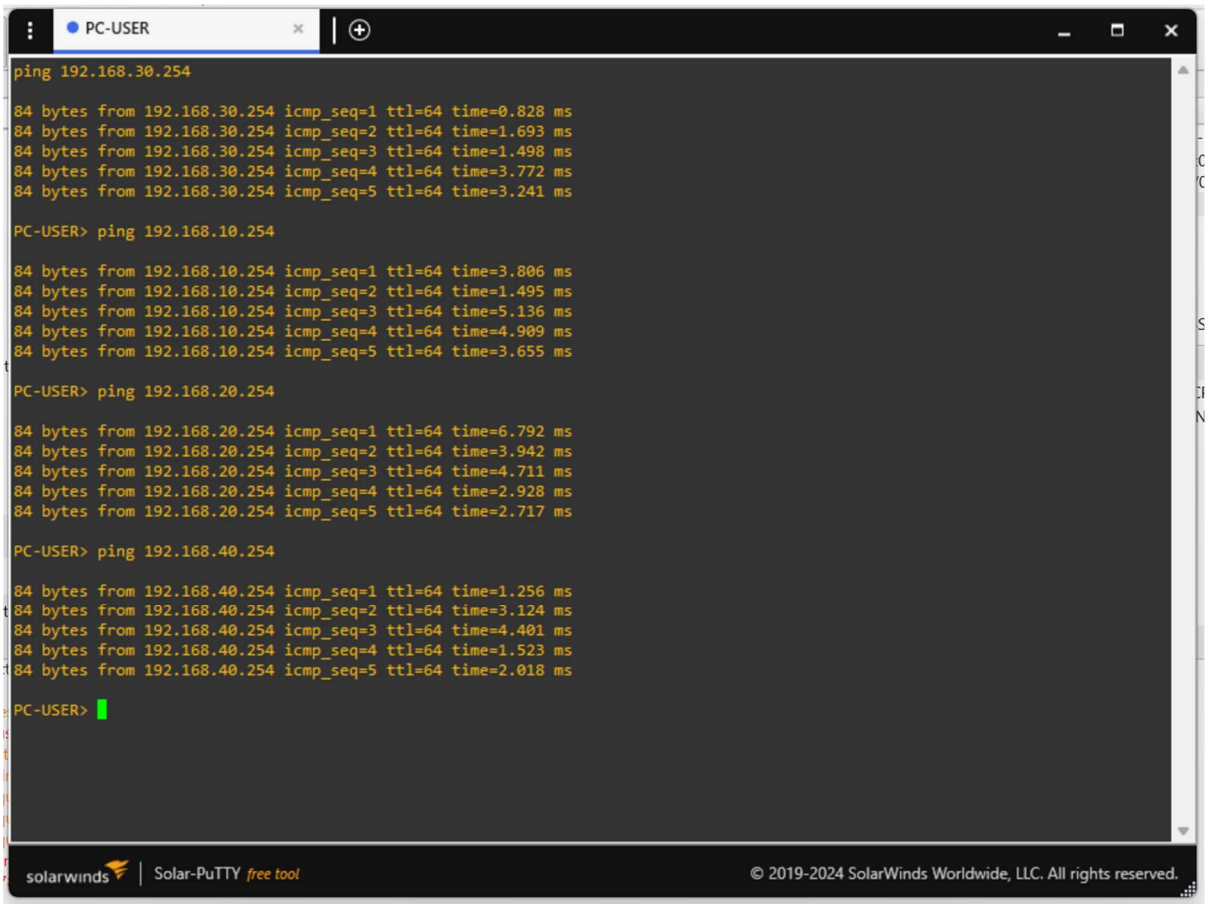


Figure 15 - Tests ping depuis PC-USER vers les passerelles VLAN

6. Synthèse des résultats obtenus

Objectif	État V1	Preuve associée
Créer les VLAN ADMIN, PRODUCTION, USERS et DMZ	Réalisé	Captures switch Cisco et pfSense VLAN
Configurer un lien trunk entre le switch et pfSense	Réalisé	show interfaces trunk sur Et0/0
Affecter les hôtes aux bons VLAN	Réalisé	Configuration des ports access et adresses DHCP obtenues
Créer les interfaces pfSense par VLAN	Réalisé	Interface Assignments pfSense
Configurer les passerelles VLAN	Réalisé	Adresses .254/24 sur les interfaces pfSense
Distribuer les adresses IP en DHCP	Réalisé	show ip sur PC-ADMIN, SRV-PROD, PC-USER, SRV-DMZ
Valider la connectivité de base	Réalisé	Tests ping vers les passerelles VLAN

La maquette V1 est donc fonctionnelle sur le périmètre réseau local segmenté. Les tests disponibles prouvent la bonne attribution IP et la communication avec les passerelles pfSense. Les règles firewall utilisées à ce stade restent des règles larges de validation technique.

7. Compétences du référentiel mobilisées

Compétence	Éléments réalisés dans ce projet
Concevoir une solution d'infrastructure réseau	Analyse du besoin, découpage en VLAN, plan d'adressage, architecture avec trunk 802.1Q et routage pfSense.
Installer, tester et déployer une solution d'infrastructure réseau	Configuration du switch, création des VLAN pfSense, assignation des interfaces, DHCP et tests ICMP.
Exploiter, dépanner et sécuriser une solution d'infrastructure réseau	Vérification des VLAN, contrôle des adresses DHCP, tests de connectivité et documentation des preuves.
Travailler en mode projet	Organisation des captures, traçabilité des étapes, documentation progressive en V1.

8. Conclusion

Cette première version de la documentation présente la mise en place de la segmentation VLAN du site principal EcoSolar Solutions. La maquette permet de séparer quatre zones réseau : administration, production, utilisateurs et DMZ. Le switch transporte les VLAN vers pfSense via un trunk 802.1Q, tandis que pfSense assure les passerelles, le DHCP et le routage de base.

Le résultat obtenu est une base d'infrastructure plus propre et plus sécurisable qu'un réseau unique. Les captures montrent que les VLAN sont créés, que les hôtes reçoivent les bonnes adresses et que les passerelles sont joignables. Cette V1 est donc exploitable comme preuve d'avancement pour l'épreuve E6.

9. Annexes - preuves et correspondance des captures

Capture	Utilisation dans la documentation
CAP_00_Dossier_Projet.png	Preuve d'organisation du dossier projet
Topologie GNS3	Présentation de l'architecture maquette
SW-CORE-ESS configuration	Ports trunk/access dans GNS3
show vlan brief / show interfaces trunk	Vérification VLAN et trunk Cisco
pfSense VLANs	Création des VLAN sur em1
pfSense Interface Assignments	Assignation des VLAN en interfaces firewall
pfSense interface ADMIN	Exemple d'adresse passerelle statique
pfSense DHCP ADMIN	Exemple de service DHCP activé
pfSense Firewall Rule	Exemple de règle de validation temporaire
VPCS show ip	Validation DHCP sur chaque VLAN
VPCS ping	Validation de la connectivité vers les passerelles

Sources utilisées

- Document de contexte EcoSolar Solutions.
- Document Projets Épreuve E6 SISR.
- Modèle de dossier projet E6.
- Captures fournies dans l'archive Projet1_ESS_Scenario1_VLAN.7z.
- Échanges de suivi de réalisation du projet.