TP VPN SITE TO SITE IPSEC

# Pré requis

2 machines 2016 avec interface graphique (expérience utilisateur) et 2 PFSENSE avec les precos suivantes

* W2016\_1 , 3 Proc virtuels, 1024 Mo de Ram, sur Switch privé LAN1, IP 192.168.10.2/24
* W2016\_2 , 3 Proc virtuels, 1024 Mo de Ram, sur Switch privé LAN2, IP 192.168.11.2/24
* PFSENSE1, 3 proc virtuels, 800 Mo de Ram, LAN sur Switch privé LAN1 Adresse 192.168.10.1/24, WAN sur Switch Privé WAN, Adresse WAN 10.0.0.1/24
* PFSENSE2 3 Proc virtuels, 800 Mo de Ram, LAN sur Switch privé LAN2 Adresse 192.168.11.1/24, WAN sur Switch Privé WAN, Adresse WAN 10.0.0.2/24

**Conseils HyperV**

Boot order

Serveur 150 Go

Pfsense désactiver le boot secure

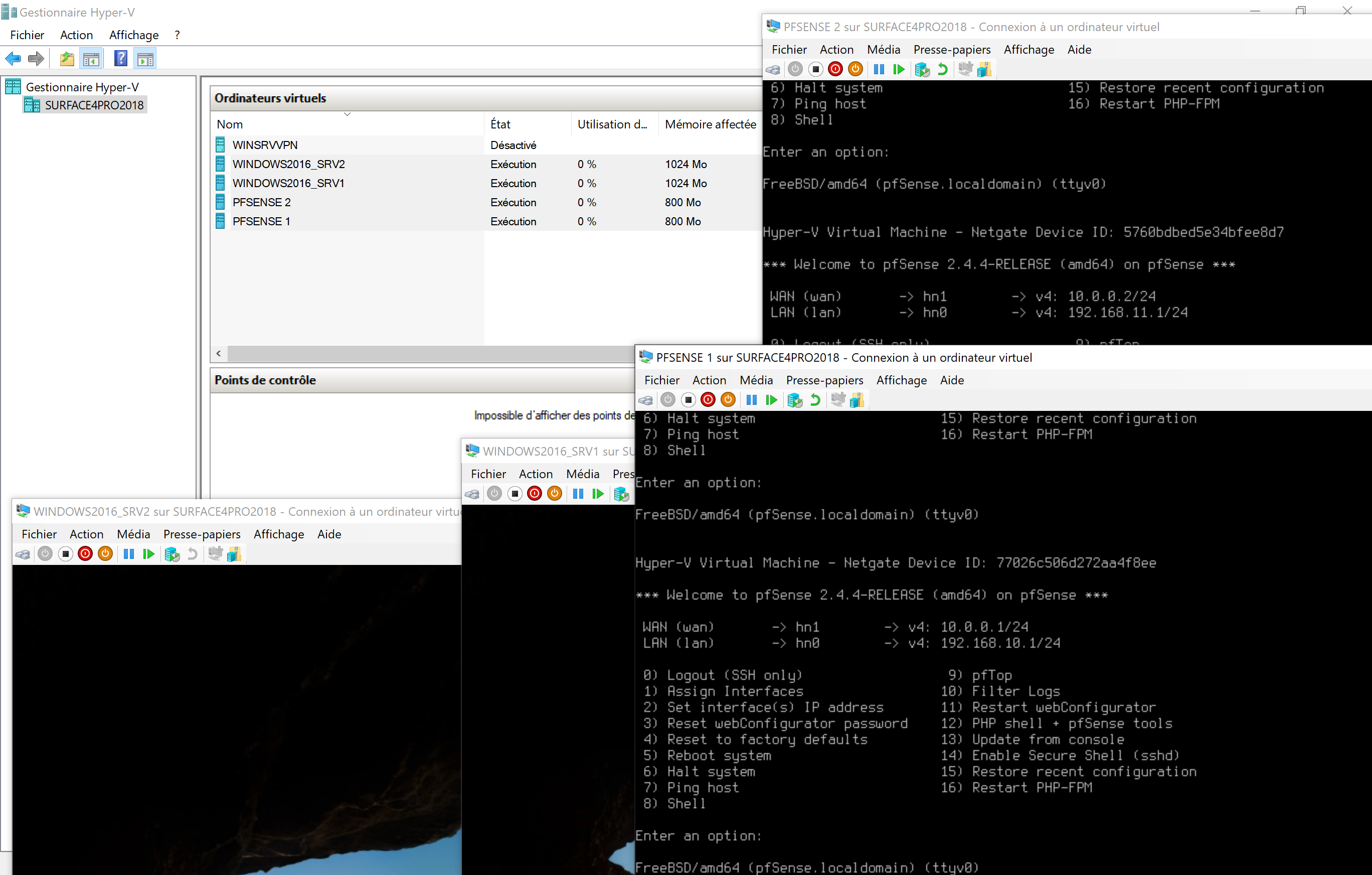
PFSENSE vous avez oublier une carte reseau avant l’install…. Choix 4 reset conf PFSense

L’ensemble de l’infra est en réseau isolé, vous n’aurez pas d’accés à internet

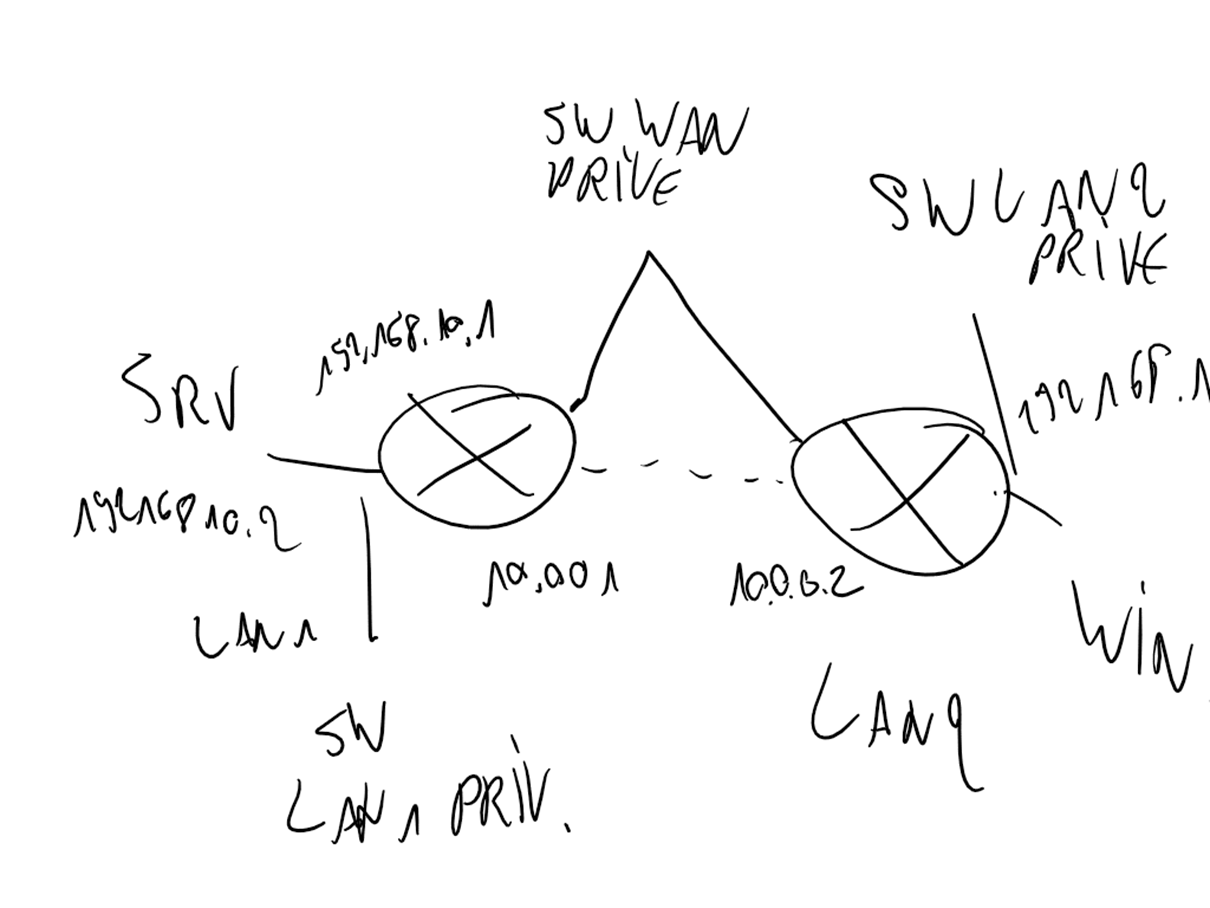
Pour les serveurs utilisez la commande sconfig pour effectuer le paramétrage IP

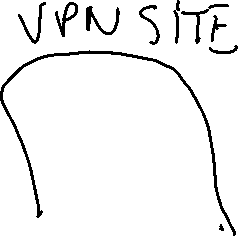
Si vous êtes en hyperv, tout en generation 2 en désactivant pour les PFSENSE le boot secure

Cette conf fonctionne sur ma surface qui possède 8 Gb de ram, donc sauf si vous avez moins de 8 Gb de Ram cela doit fonctionner, la preuve sur ma surface 4 i5 8 Gb 256 SSD



Voici un schéma basique de l’infra





# Référence CISCO

# TACHES A EFFECTUER

DEBLAECKER JEREMY \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

N’oubliez pas de renommer le doc avec vos noms et prénoms

Mettre un screen de votre progression à chaque tache directement sur ce document

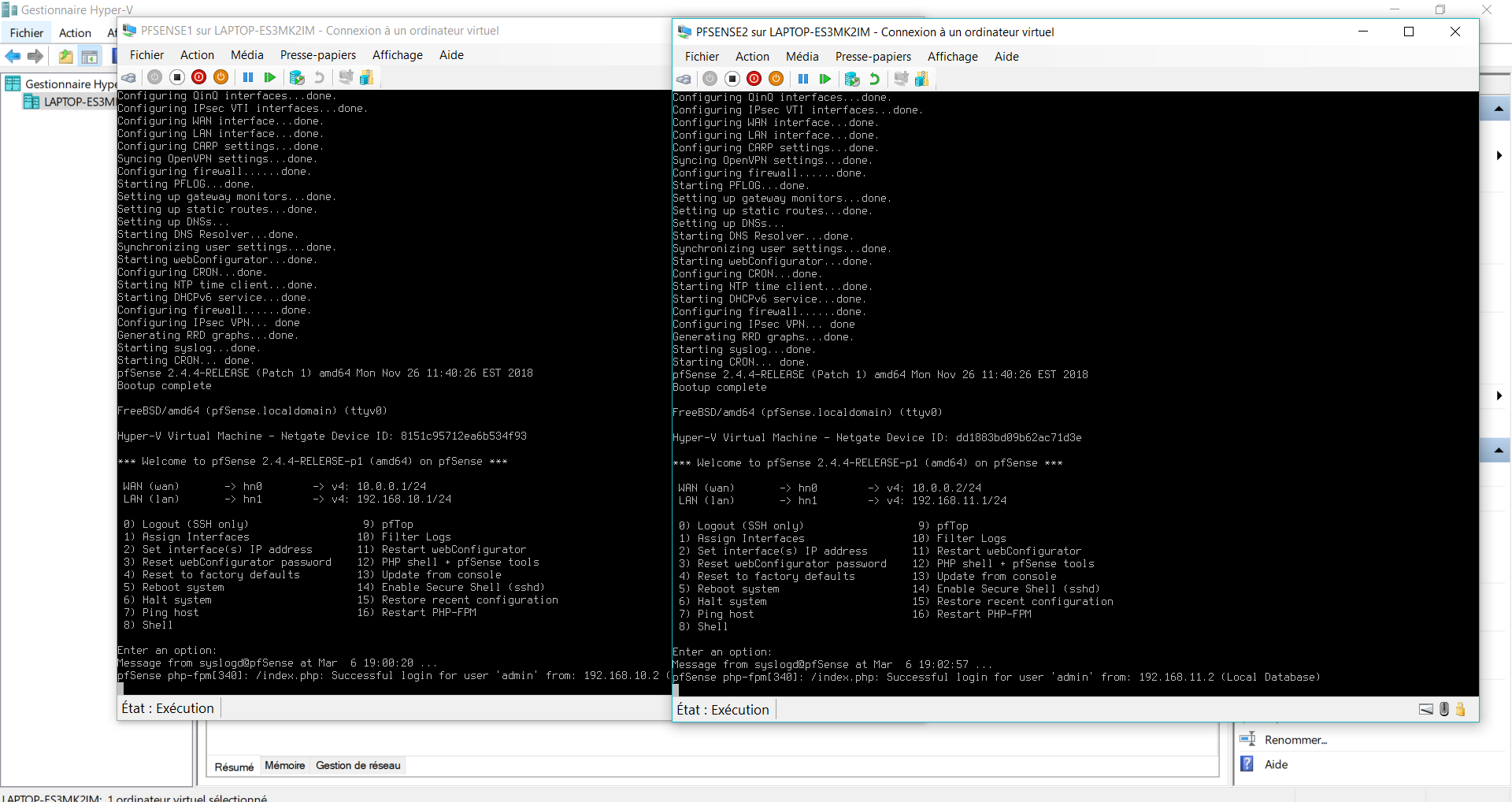
## Suppression des tables de routage

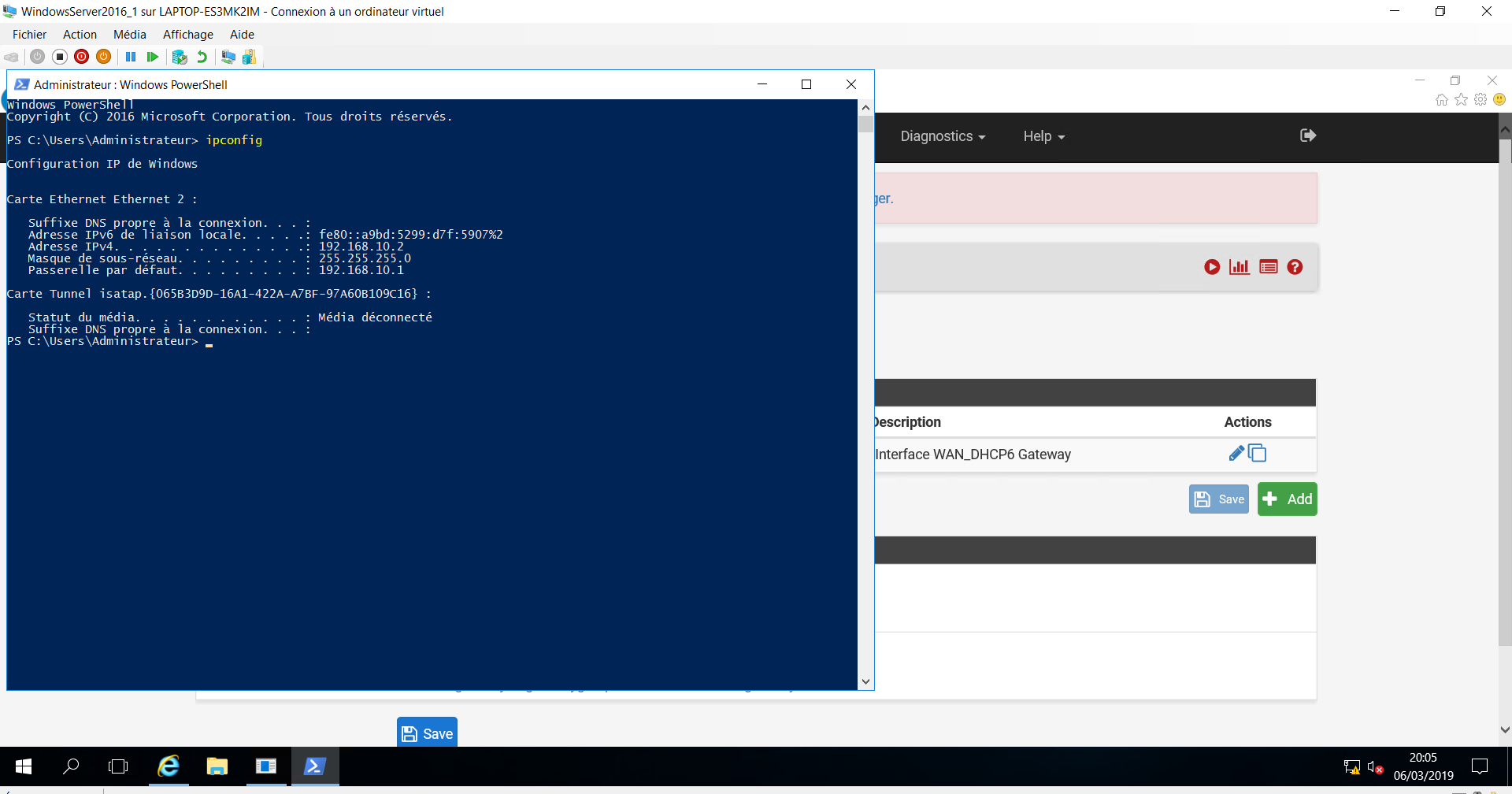
Sur chaque PFSENSE supprimer ou désactiver les tables de routage du précédent TP

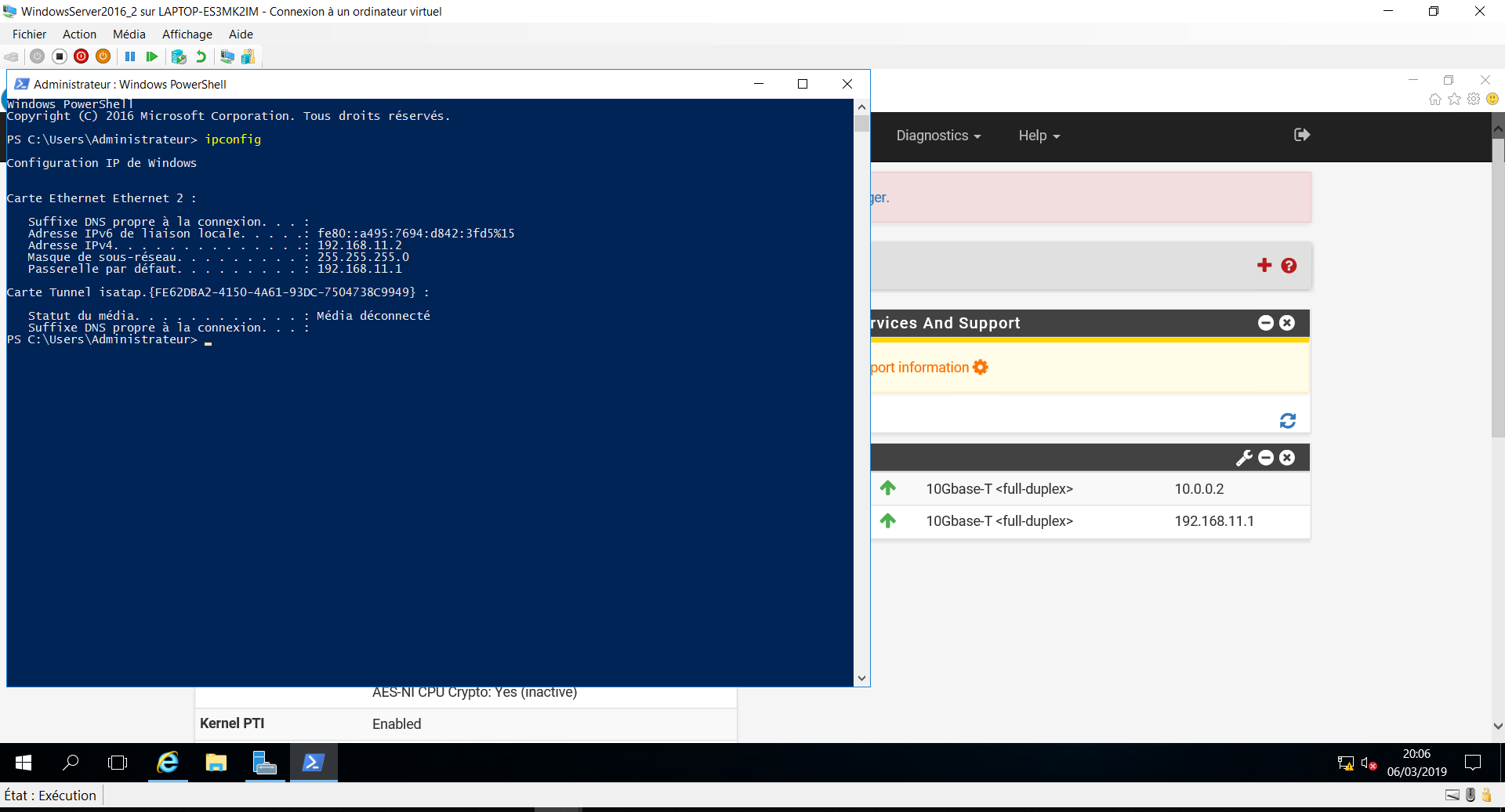
Une image contenant capture d’écran

Description générée automatiquement

## Vérification de l’infra demandée







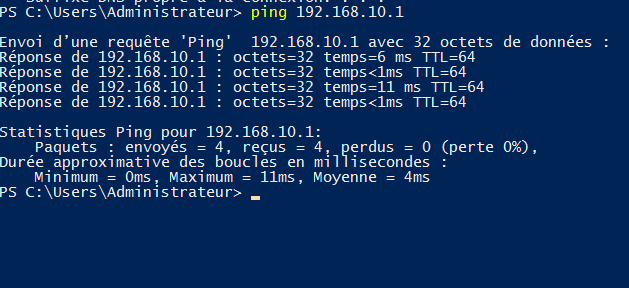
(Screen des VM + adressage réseau)

## Test de connectivité

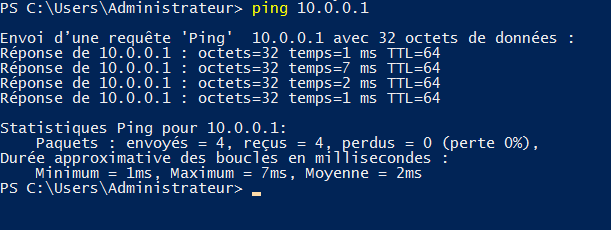
A partir de chaque serveur, tester la passerelle et l’ipwan du routeur, mettre un screen à chaque fois. Vérifier les règles de pare feu de PFSENSE le cas échéant.

**Ping qui doivent fonctionner (screens)**

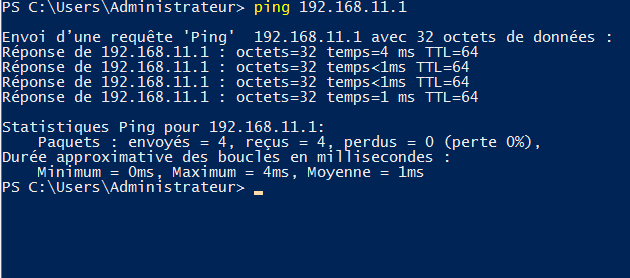
**SRV1 VERS PASSERELLE 1**



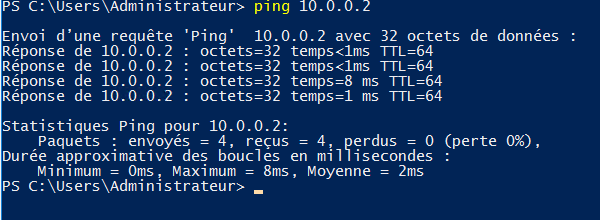
**SRV1 VERS IPWAN 1**



**SRV2 VERS PASSERELLE 2**

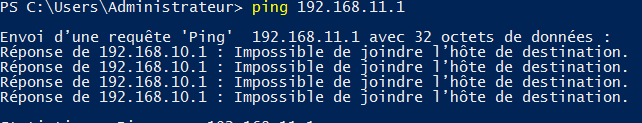


**SRV2 VERS IP WAN 2**

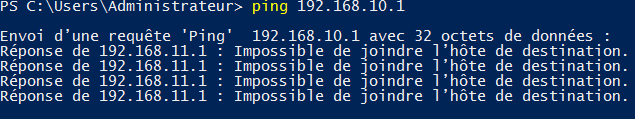


**Ping qui doivent échouer (screens)**

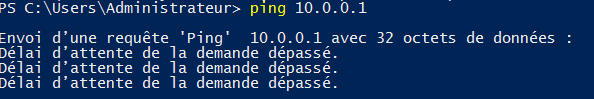
**SRV1 vers IP LAN SRV 2**



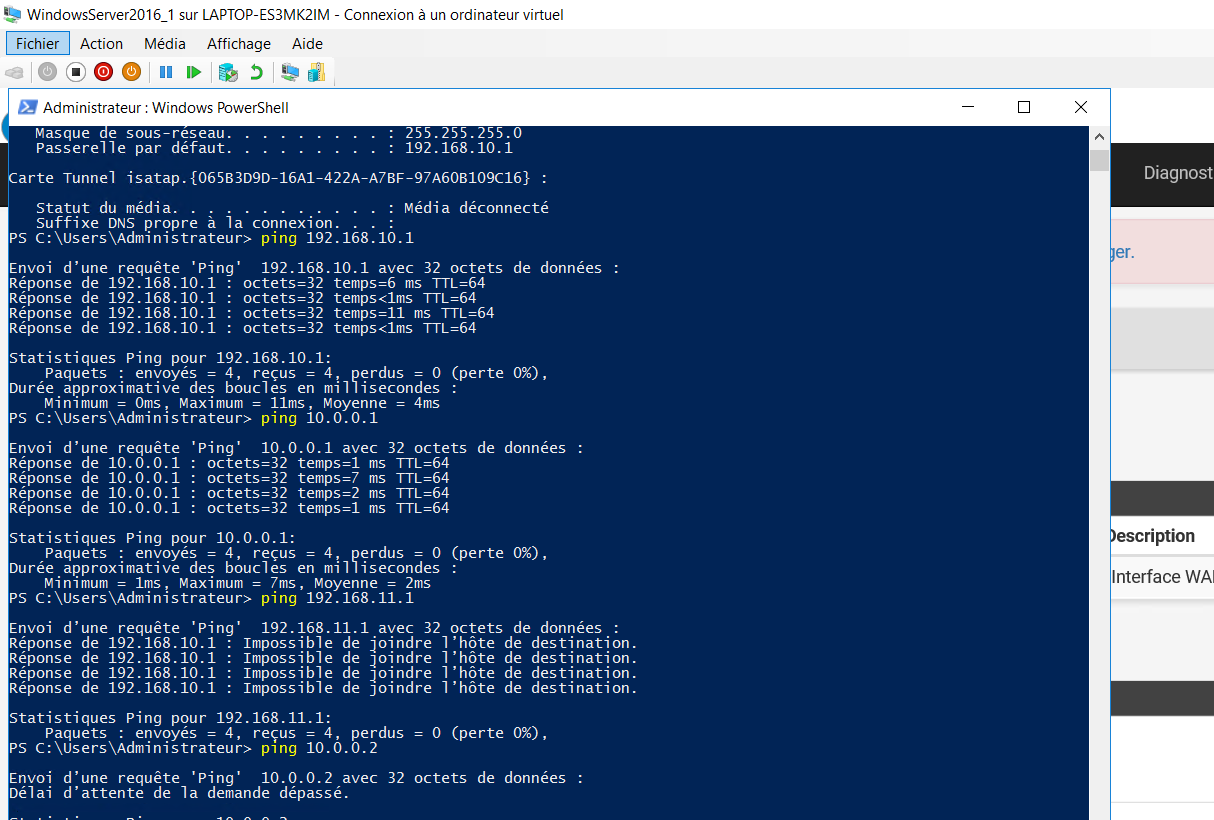
**SRV2 vers IP LAN SRV 1**



**SRV2 VERS IP WAN 1**



**SRV1 vers IPWAN 2**

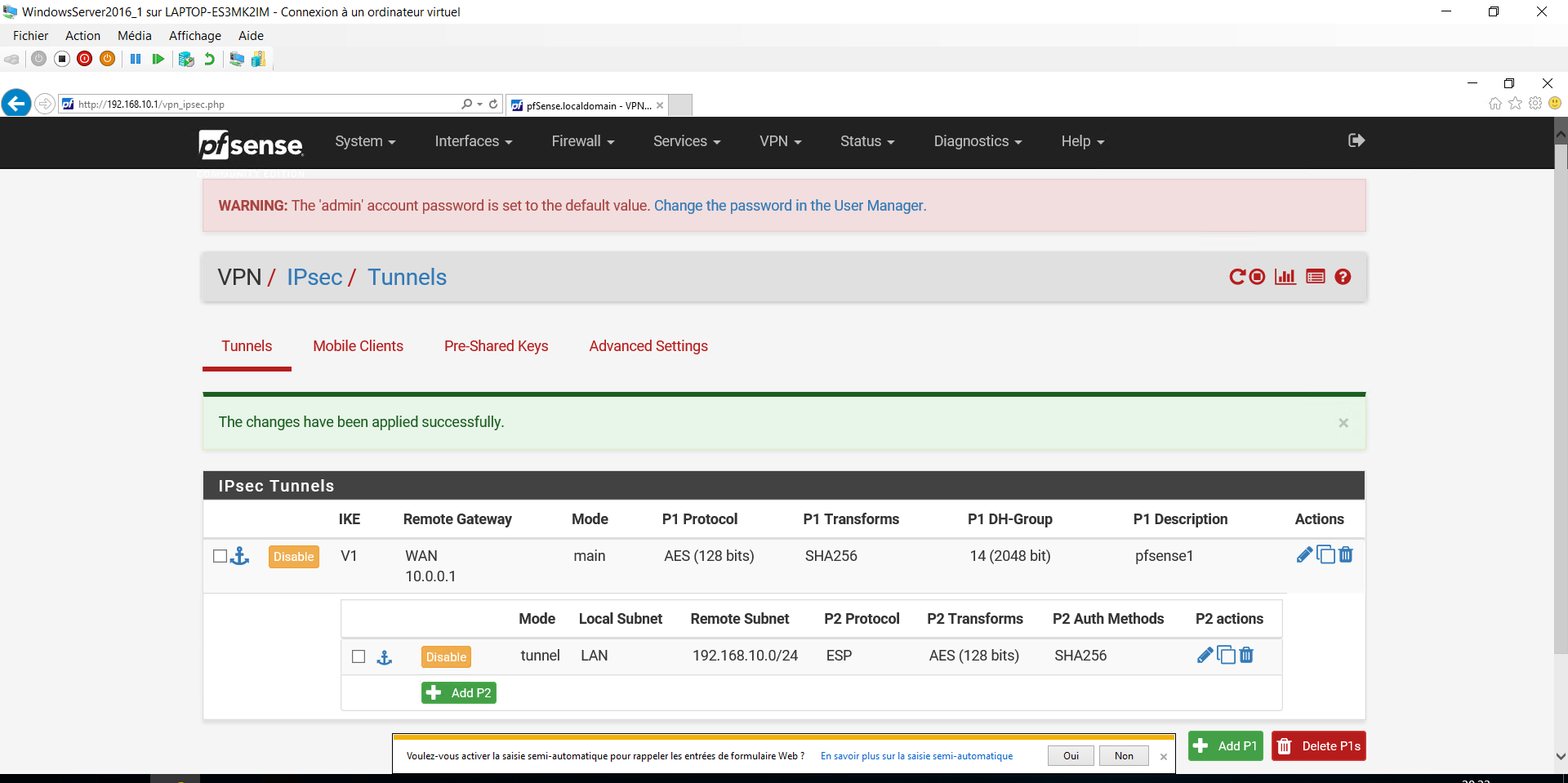


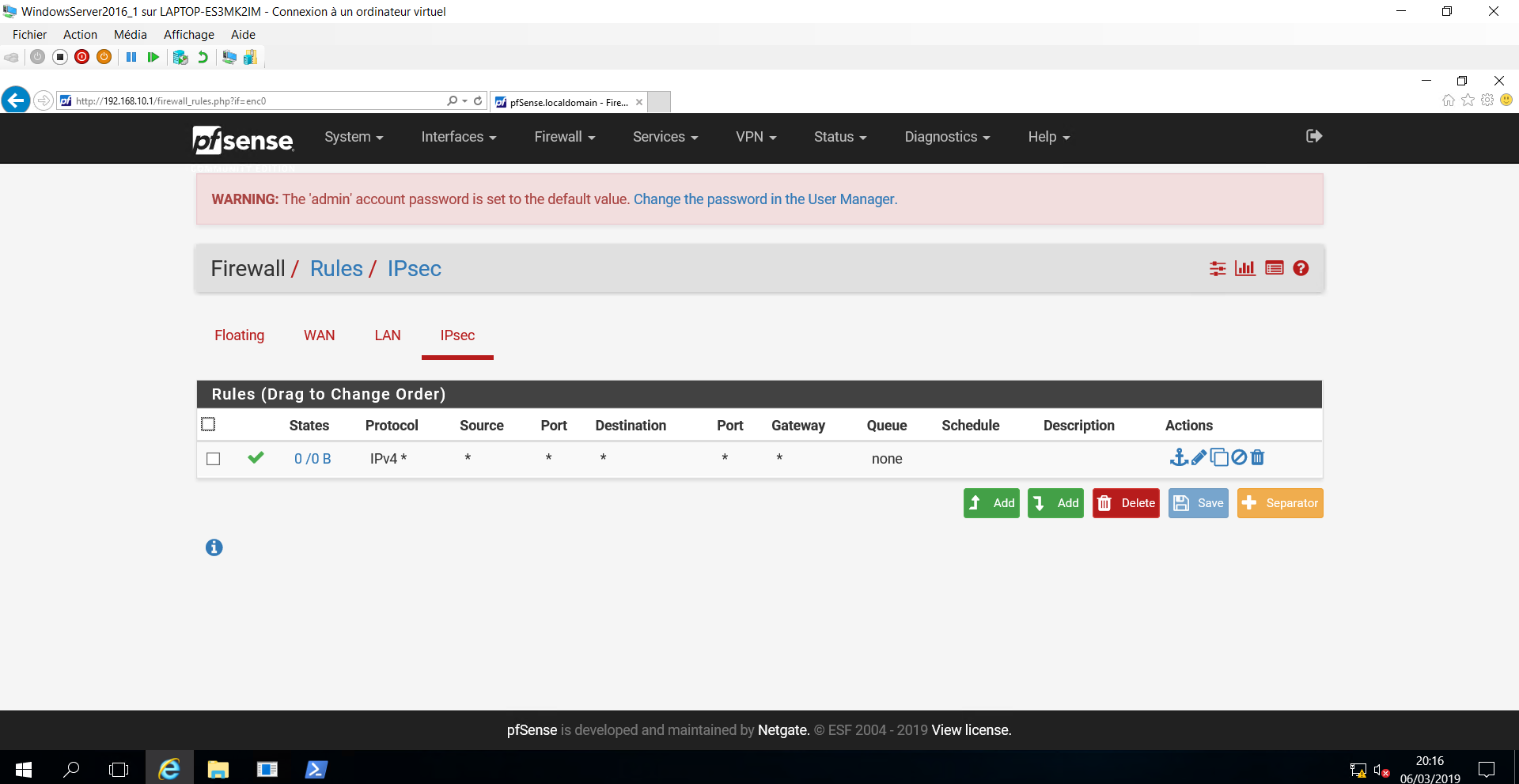
## TRACERT

**Faire pareil avec TRACERT**

## METTRE EN PLACE EN SUIVANT LE TUTO ET EN UTLISANT L’ADRESSAGE IP DE CE TP, UN VPN IPSEC SITE TO SITE entre les 2 routeurs

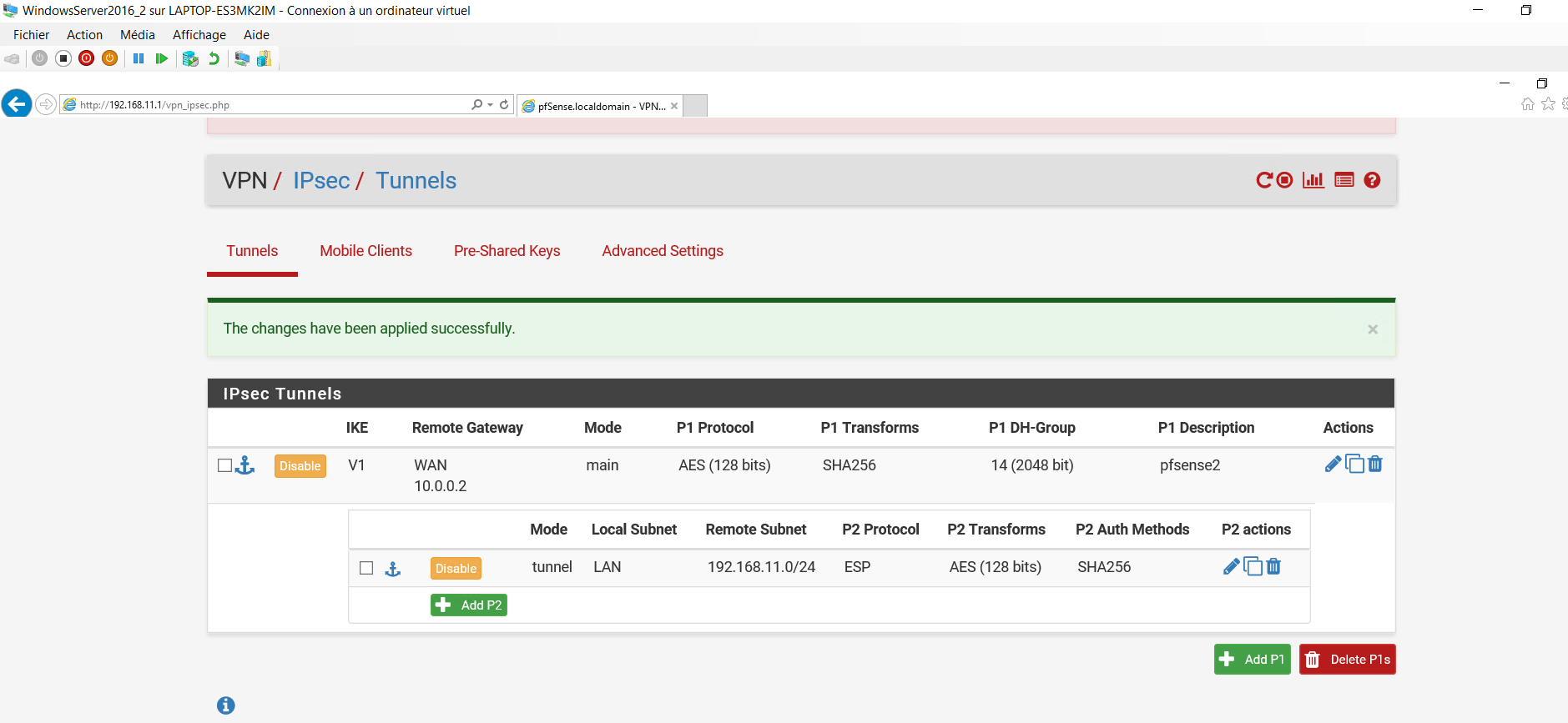
PFSENSE1

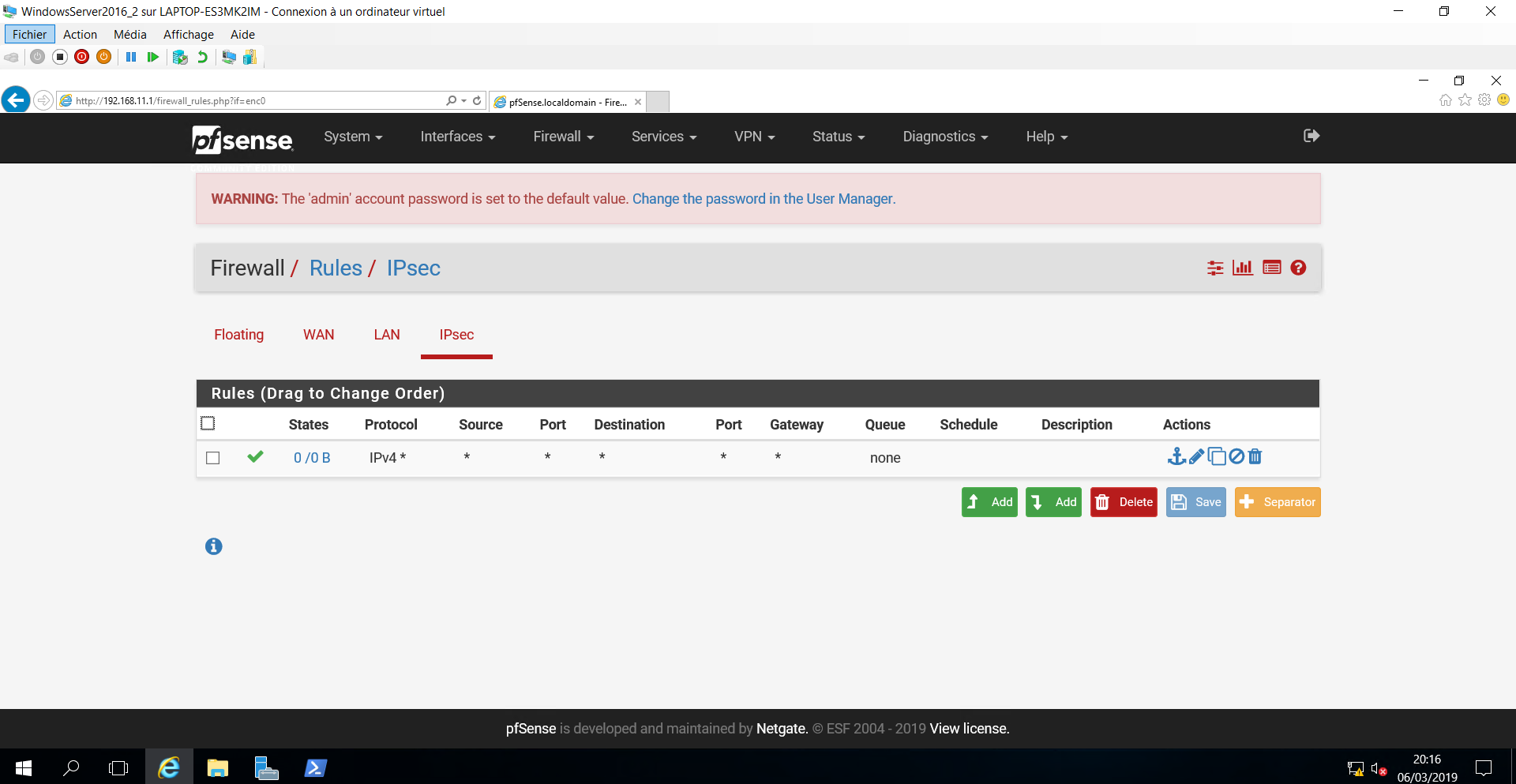






PFSENSE2







## TEST DE DECONNEXION

Déconnecter le VPN SITE TO SITE, faire un ping du SRV 1 à partir du SRV2

Que constatez vous ?

(screen \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*)

## PARTAGE SMB

A partir du serveur 1, dans l’explorateur tapez :

[\\IP](file:///\\IP) DU SRV 2\C$

Que constatez vous ?

(screen \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*)

## TEST DE CONNECTIVITE

**Ping qui doivent réussir (screens)**

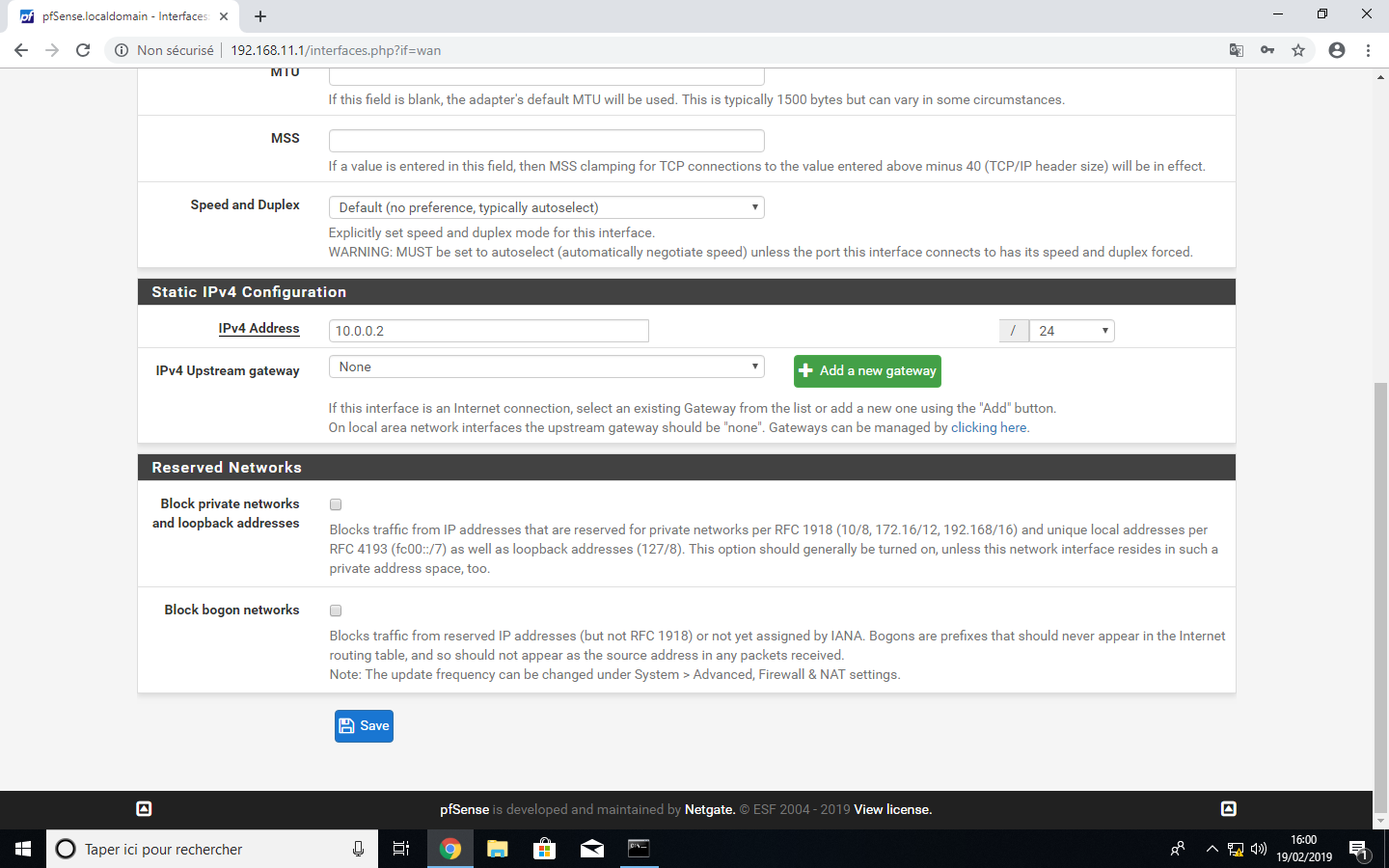
**SRV1 vers IP LAN SRV 2**

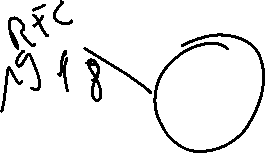
**SRV2 vers IP LAN SRV 1**

Faire de même avec TRACERT

# ATTENTION

Attention, il faut désactiver la RFC 1918 pour ce TP





PFSENSE INTERFACE WEB PFSENSE

Login admin

Mdp pfsense

GESTIONNAIRE DE SERVEUR Désactiver la configuration renforcée d’IE