

**FILIERE : GENIE CYBER DEFENSE ET SYSTEME DE TELECOMMUNICATION EMBARQUEES**

**TP : Technologies de VLAN EN GNS3**

##### **Réalisé par :** **Encadré par :**

ELOUARDI Saida M. Youssef khaoulaj

M. Anas ABOU EL KALAM

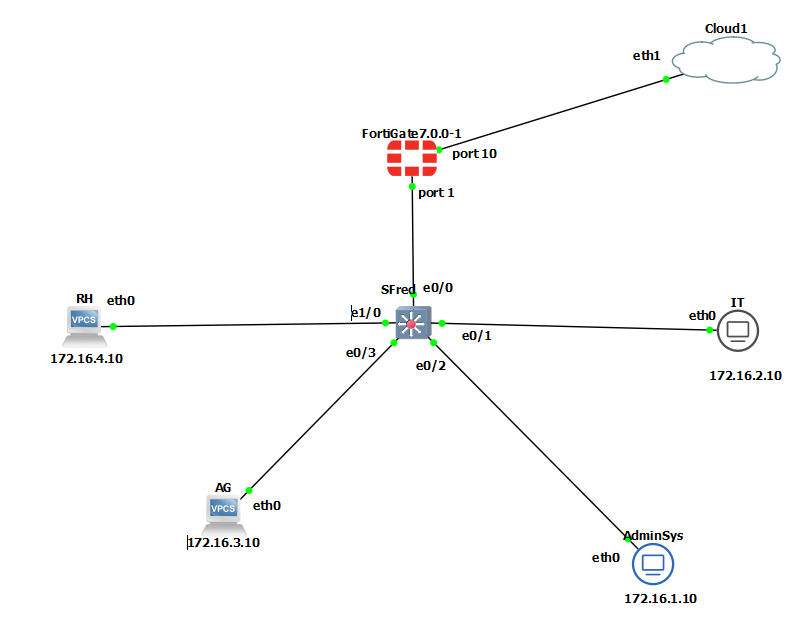
**Année Universitaire : 2022-20Objectif :**

***Objectif :***

Au cours de ce TP, notre objectif est d'établir un schéma au sein du laboratoire GNS3 afin de déployer des VLANs, de les interconnecter avec un pare-feu FortiGate, de les lier à un réseau WAN, et d'implémenter le routage inter-VLAN.

Un VLAN (Virtual Local Area Network) offre la possibilité de segmenter de manière logique un réseau local (LAN) en différents domaines de diffusion. Lorsque des données sensibles risquent d'être diffusées sur un réseau, la création de VLANs permet d'améliorer la sécurité en assignant une diffusion spécifique à un VLAN particulier. Ainsi, seuls les utilisateurs faisant partie d'un VLAN donné peuvent accéder aux données de ce VLAN et les manipuler.

Voici notre architecture à réaliser :



**VLAN 99 AdminSys**: 172.16.1.0/24

**VLAN 2 IT:** 172.16.2.0/24

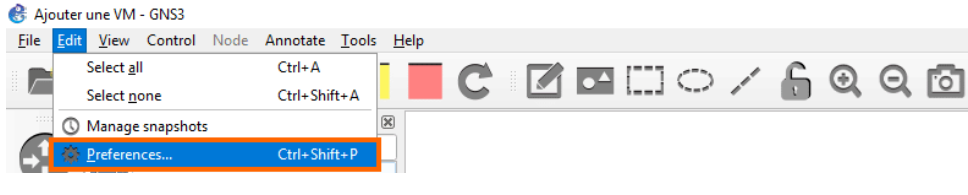
**VLAN 3 AG:** 172.16.3.0/24

**VLAN 4 RH**: 172.16.4.0/24

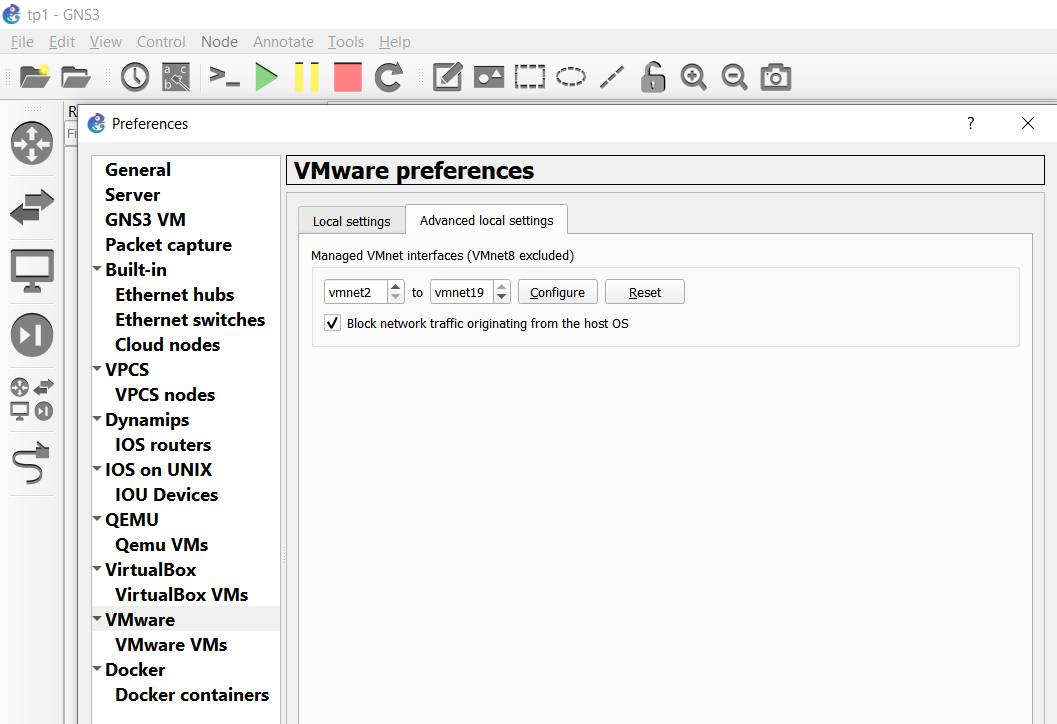
**Configuration de L’environnement de travail de GNS**

1. **Importer les machines virtuelles**

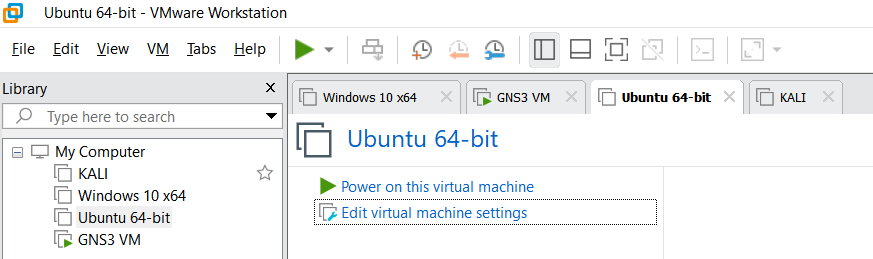
Dans GNS3, nous nous rendrons dans le menu « **Edit**» puis « **Préférence**».

Nous nous rendrons dans le menu latéral « **VMWare**» puis nous sélectionnerons l’onglet «**Advanced Local Settings** ». Il nous faudra autant de «**VMnet interface** » que de machine virtuelle à importer dans GNS3. **Dans cet exemple, nous créerons 18 VMNet de 2 à 19.**

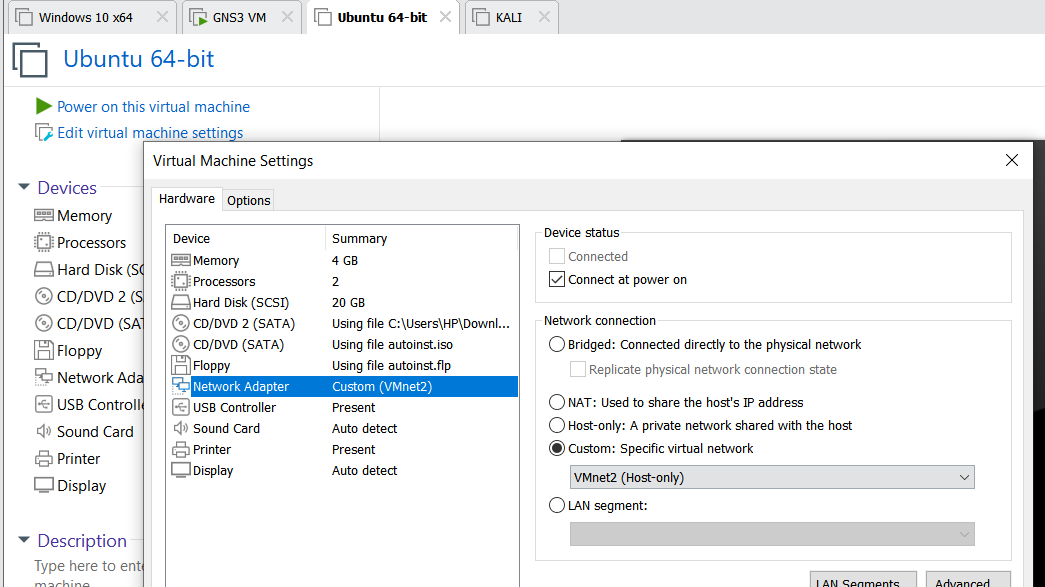
Dans les listes déroulantes, nous sélectionnerons la première et la dernière VMNet, puis nous cliquerons sur le bouton « **Configure**». Une invite de commande se lance et crée les adaptateurs réseaux sur la machine principale qui héberge la plateforme GNS3. Nous confirmerons la création de cette carte réseau en cliquant sur le bouton « **Apply**» puis sur « **OK**».



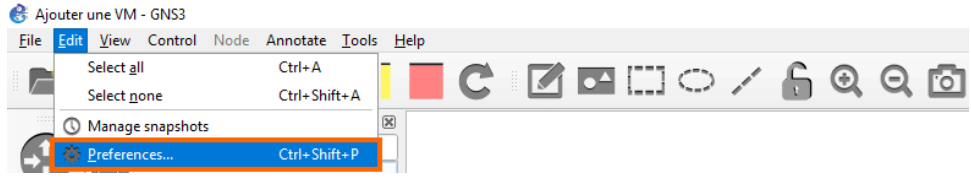
Une fois la machine virtuelle éteinte, nous allons nous rendre dans les paramètres de la machine virtuelle, en cliquant sur l’option « **Edit virtual machine settings** ».



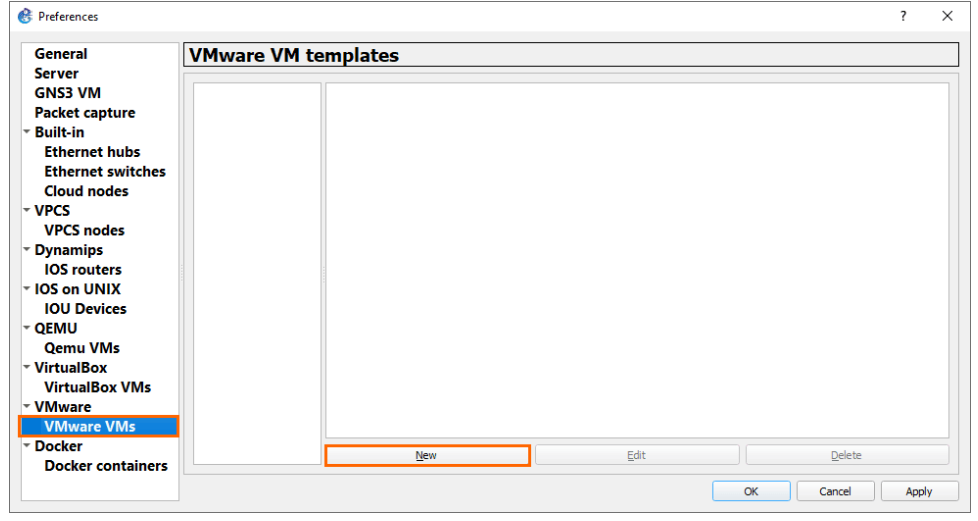
Nous sélectionnerons « **Network Adaptater**» dans la section « **Hardware**» puis dans la partie de droite, nous opterons pour l’option « **Custom**» et nous sélectionnerons un VMNet créé dans GNS3 (souvenez-vous de la liste de VMNET2 à VMNET6). Dans cet exemple, **VMNET2**.



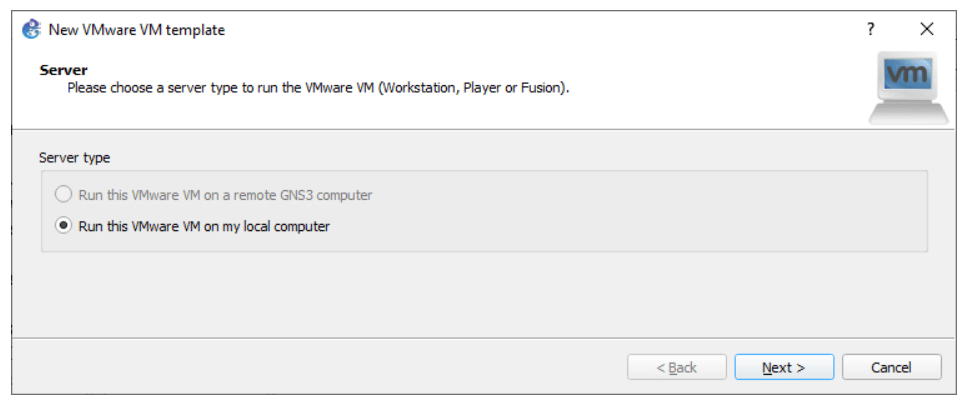
**Notre machine est maintenant prête à importer dans GNS3.** Dans GNS3, nous allons nous rendre dans le menu déroulant « **Edit**» puis « **Preference**».



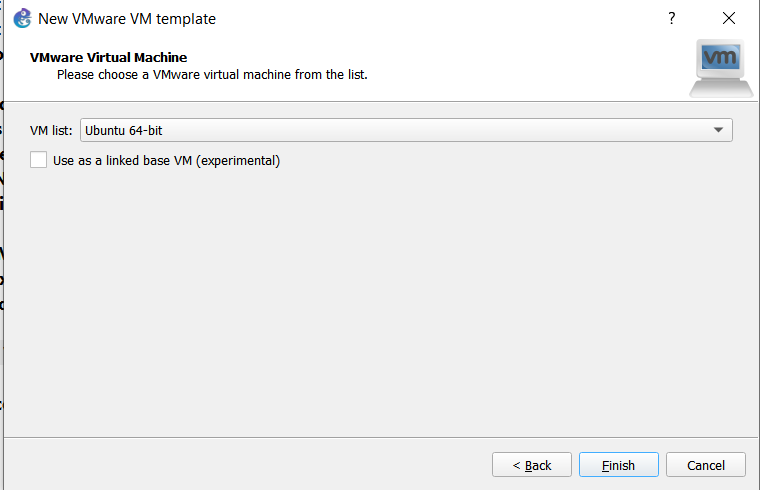
Le menu latéral, nous sélectionnerons « **VMware VMs**» puis nous cliquerons sur le bouton « **New**».



Nous lancerons ainsi l’assistant d’importation de la machine virtuelle. La première étape, nous indiquerons où sera exécutée la machine virtuelle. Dans une configuration de base, nous n’avons pas d’autre choix que d’**exécuter la machine virtuelle sur la machine locale**. Nous cliquerons sur le bouton donc sur le bouton « **Next**».



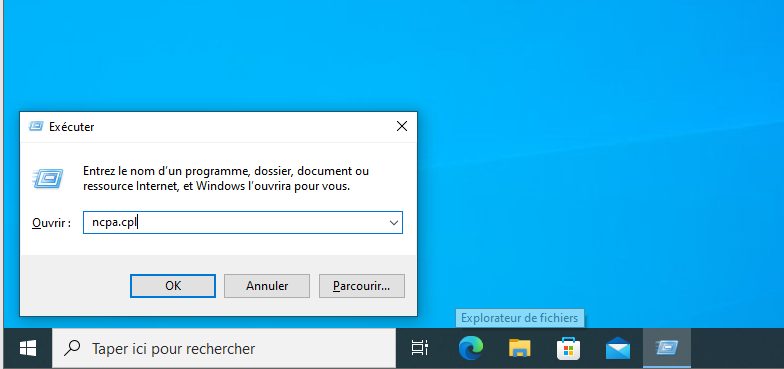
Dans la liste déroulante, **nous sélectionnerons la machine virtuelle que nous souhaitons importer**, à savoir notre VM "ubuntu64-bit", puis nous validerons notre choix en cliquer sur « **Finish**».



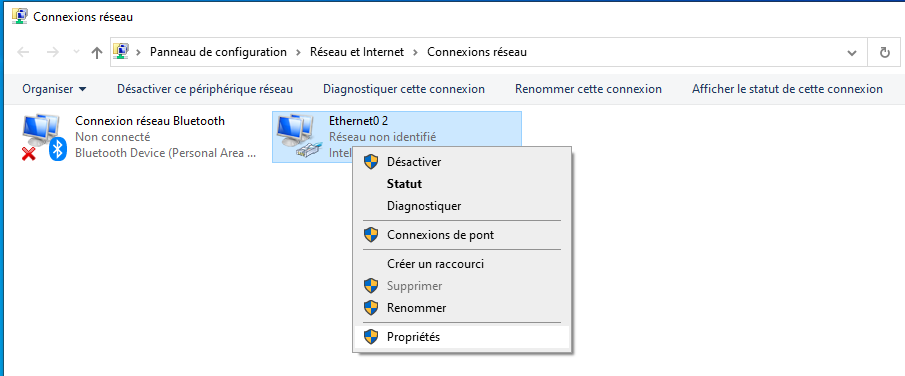
1. **La configuration machine virtuelle IT en utilisant le système d'exploitation Windows.**

Pour accéder à la machine virtuelle, il nous faudra nous rendre sur VMWare Workstation**.**

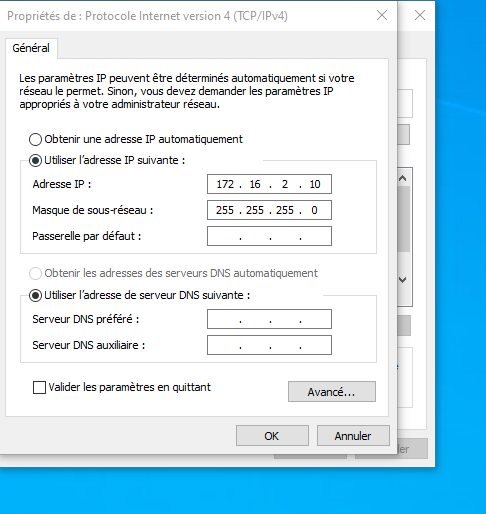
Nous modifierons**la configuration réseau au sein du système d'exploitation Windows 10 de la VM**. Nous accéderons à la fenêtre « **Exécuter** » de notre machine virtuelle à l’aide du raccourci clavier [WINDOWS] + [R]. Nous ouvrirons la console de configuration réseau « **ncpa.cpl** ».



Nous allons modifier les paramètres de la configuration réseau. Dans le menu contextuel, nous sélectionnerons l’option « **propriétés**».

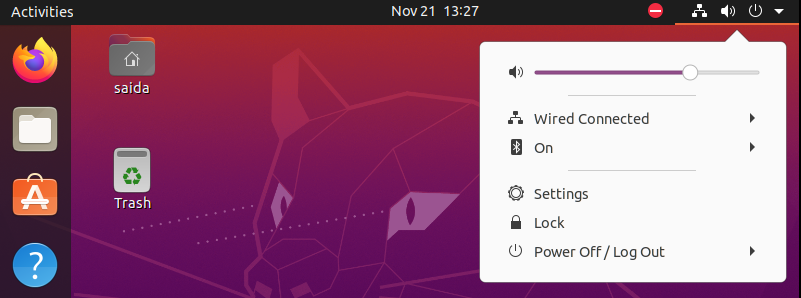


De retour sur la fenêtre des propriétés de la carte, nous pouvons cliquer sur le bouton « **Fermer**».

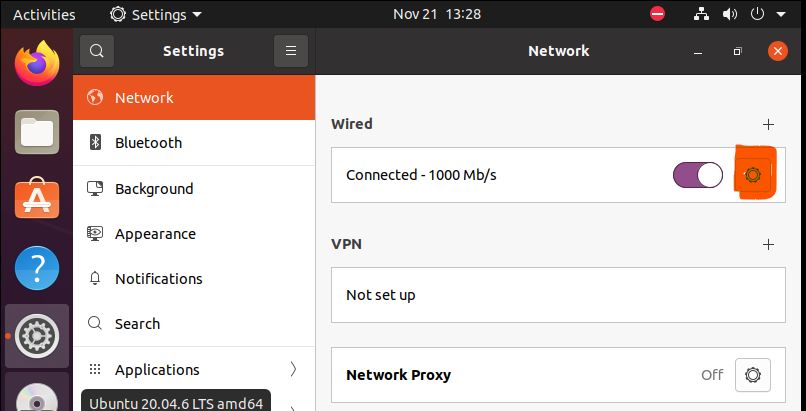


1. **La configuration machine virtuelle**

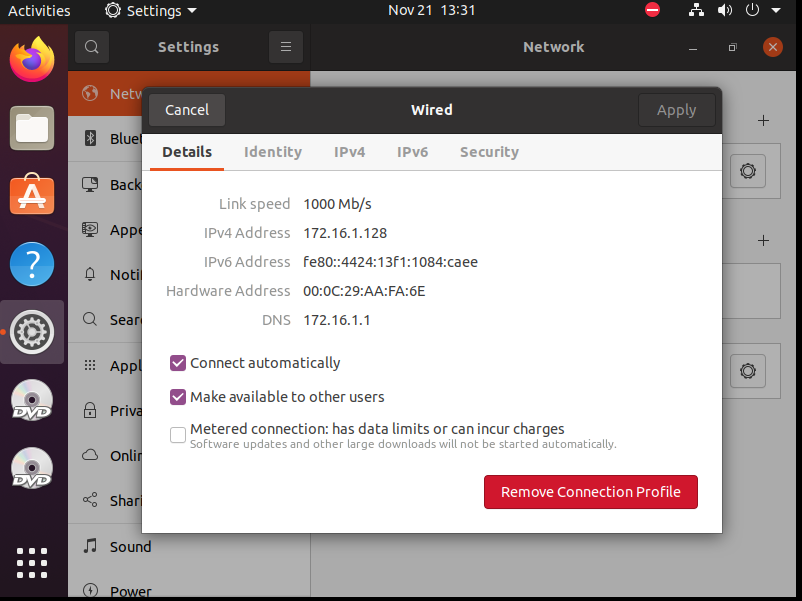
Ouvrez les paramètres d’Ubuntu en cliquant sur l’icône ampoule en haut à droite de l’écran.  
Puis cliquez sur Paramètres.



Ensuite à gauche, cliquez sur Réseau, Puis sur l’interface réseau filaire ou Wifi, cliquez sur l’icône roue crantée

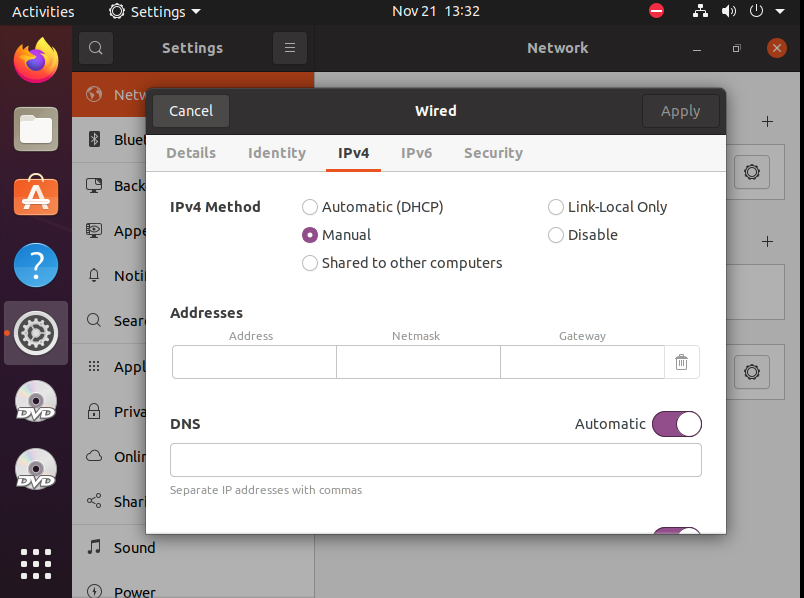


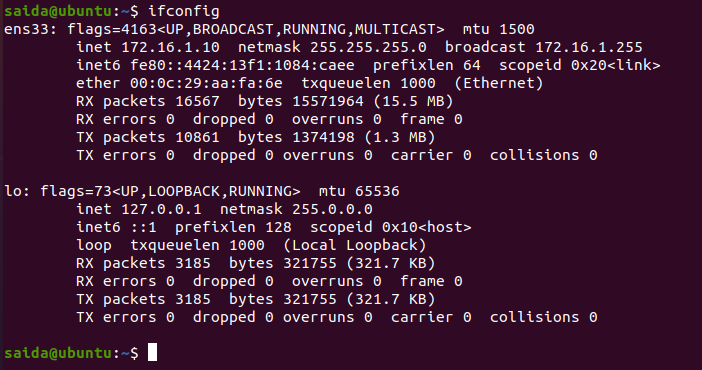
Ensuite, on arrive sur les paramètres de l’interface réseau, On y trouve un onglet IPv4 et IPv6 afin de configurer [**les paramètres TCP/IP**](https://www.malekal.com/le-protocole-tcp-ip-definition-architecture-et-couches/) de ces derniers.  
Au besoin lire :



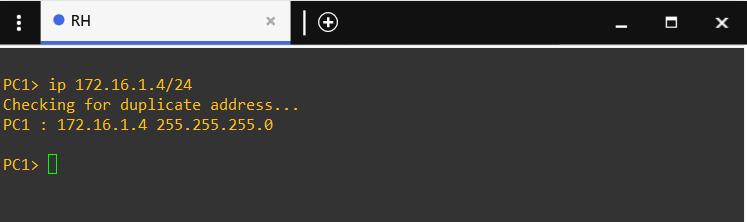
Ci-dessous les paramètres IPv4 :

* **Méthode IPV4** : c’est la méthode d’attribution IP – automatique DHCP ou manuel  
   On peut alors configurer une ou plusieurs adresses IP avec [le masque de sous réseau](https://www.malekal.com/le-masque-de-sous-reseau-ou-netmask-dans-adressage-tcp-ip/) et la passerelle.
* Ensuite cliquez en haut à droite sur le bouton **Appliquer** afin de prendre en compte les modifications.

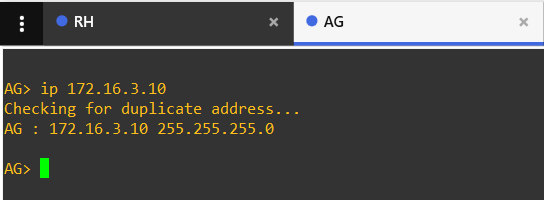




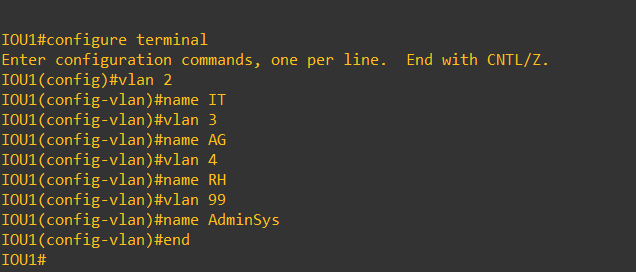
* **Configuration des machine RH :**

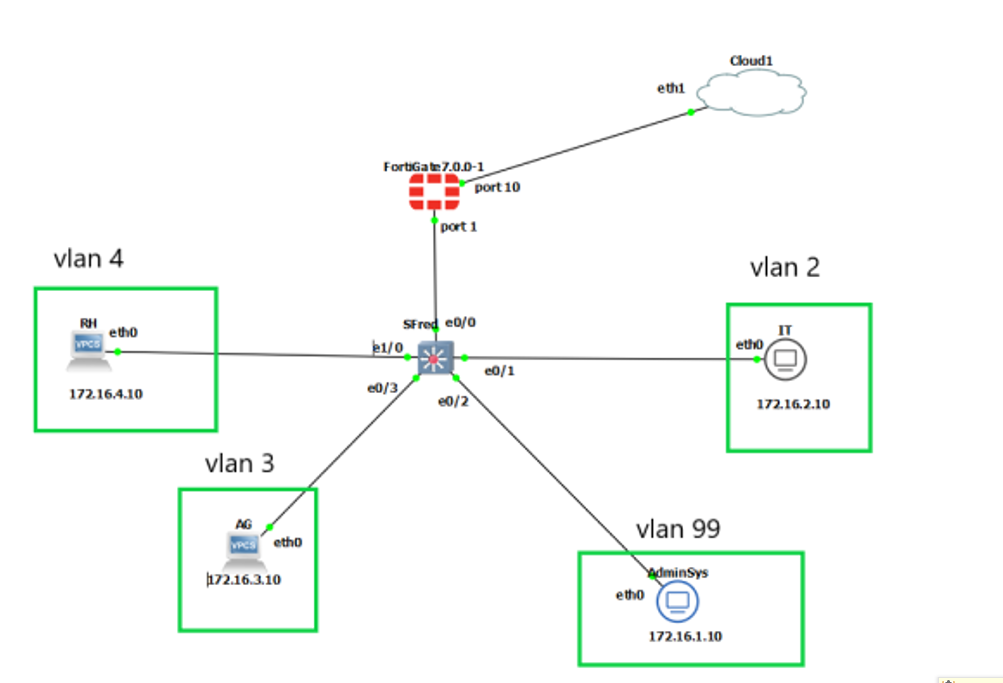


* **Configuration de machine AG**

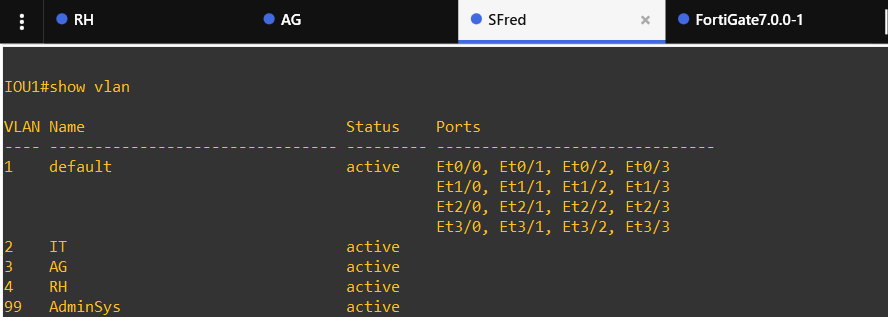


1. **Création de vlans VLAN 2 ; IT, VLAN 3 ; AG, VLAN 4 ; RH et VLAN 99 AdminSys. Sur SFed**

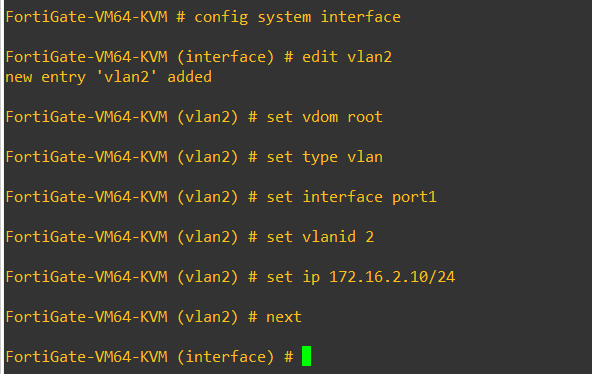


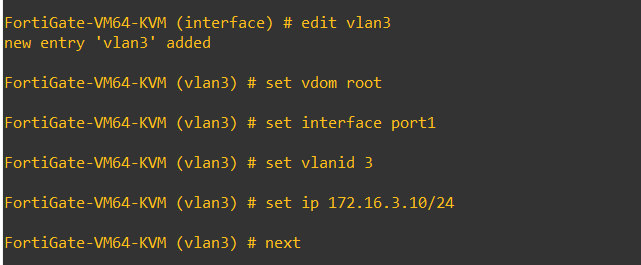


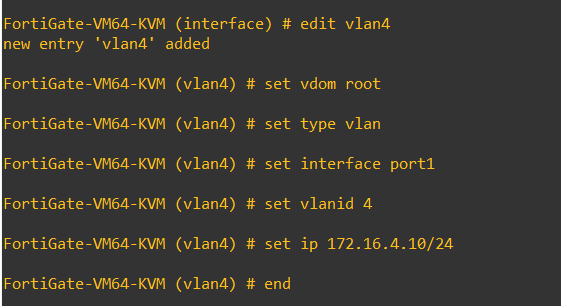
Pour s’assurer des VLANS qu’on a créé, on les affiche avec la commande show vlan :

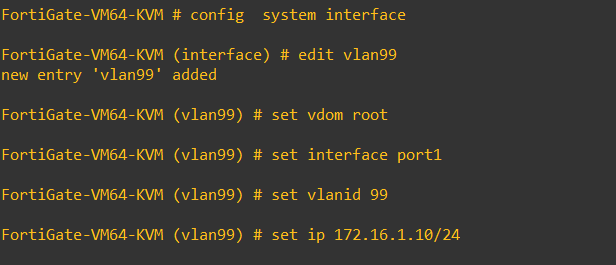


**3.1 Création des VLANS sur le Firewall**

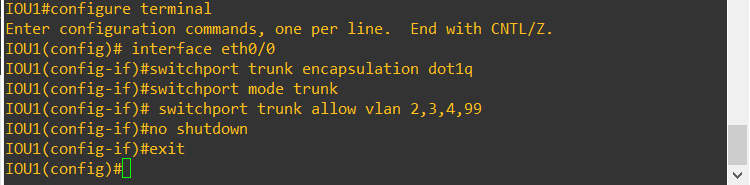




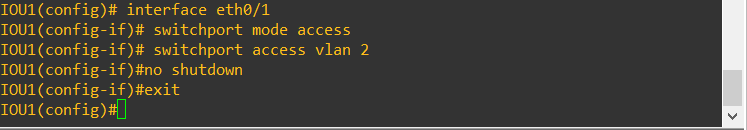




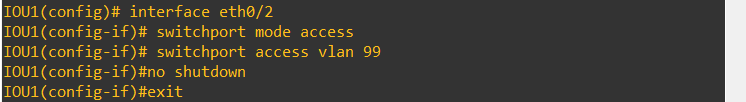
**4.Configuration du port 1 d'interconnexion Switch-Pare-feu en mode multi-VLAN”**



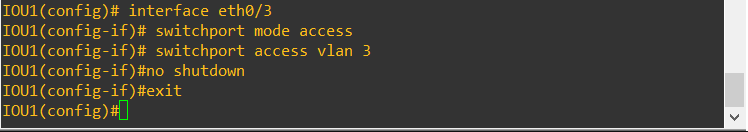
* 1. **Configurez le port de la machine IT sur le switch SFed sur le vlan 2**



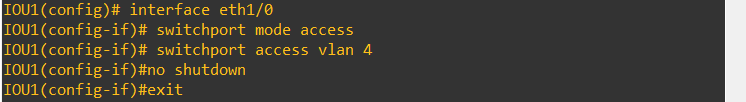
* 1. **Configurez le port de la machine AdminSys le switch SFed sur le vlan 99**



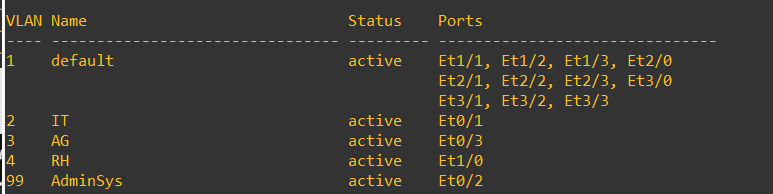
* 1. **Configurez le port de la machine IT le switch SFed sur le vlan 3**



* 1. **Configurez le port de la machine IT le switch SFed sur le vlan 3**

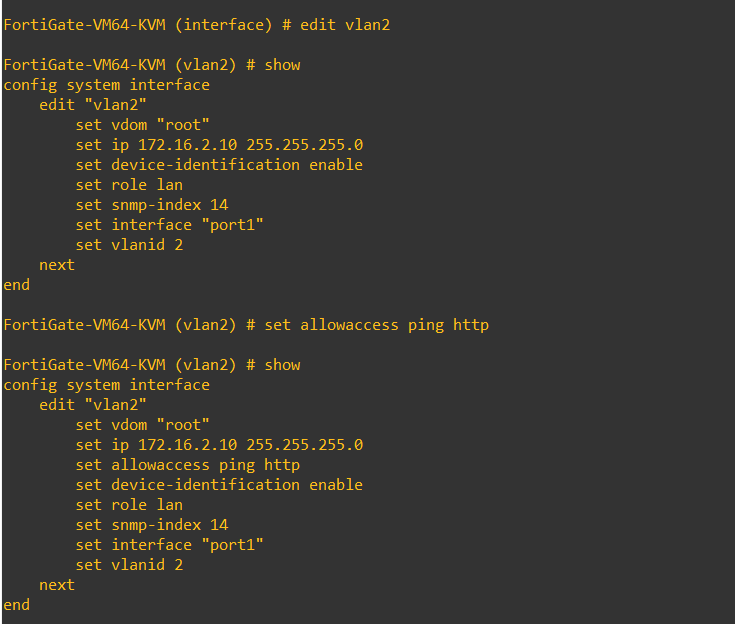


Voilà ainsi notre configuration finale des ports sur les différents VLANS

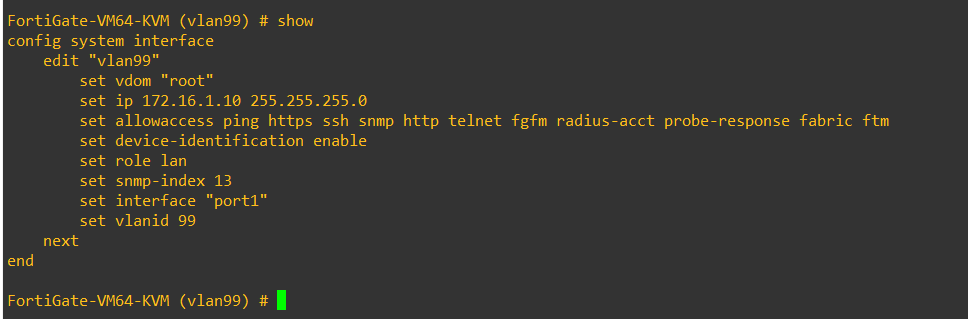


**6.1 Autorisation des protocoles sur les VLANS**

Autorisation des protocoles sur les VLANS L’autorisation des protocoles se fait au niveau du Firewall Fortigate CLI, et aussi dans la versionWebdeFortigate en sélectionnant les protocoles qu’on veut autoriser par la suite

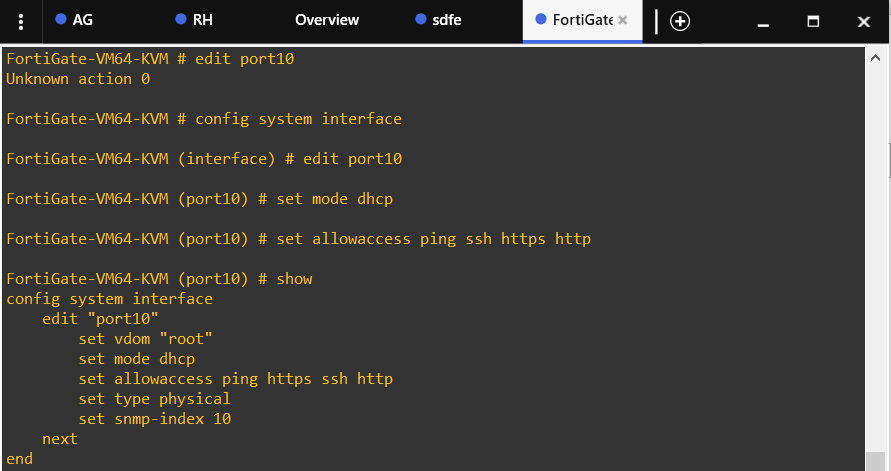


De même pour autoriser tous les protocoles pour le VLAN AdminSys.

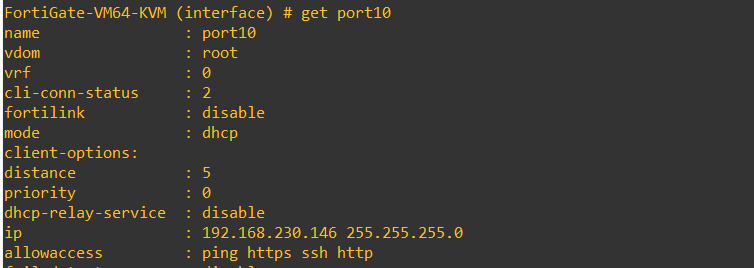


**6**.**2 Accéder à l’interface web du pare-feu FTG**

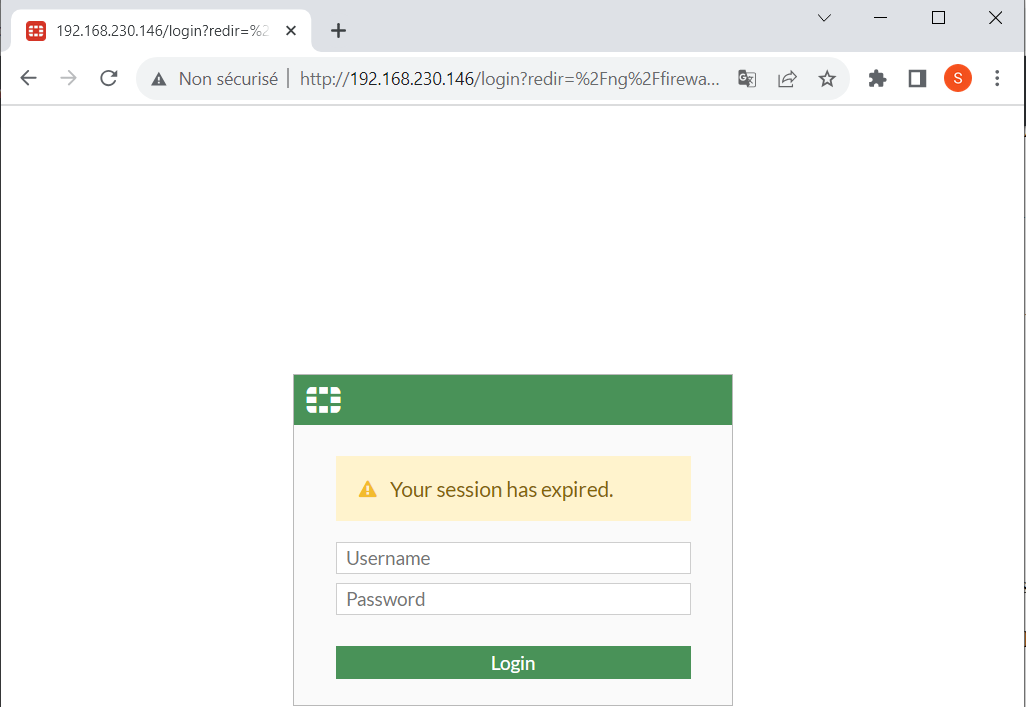
On a en effet configuré l'interface pour utiliser DHCP afin d'obtenir son @IP et ses paramètres réseau de manière dynamique plutôt que d'attribuer une @ IP statique.



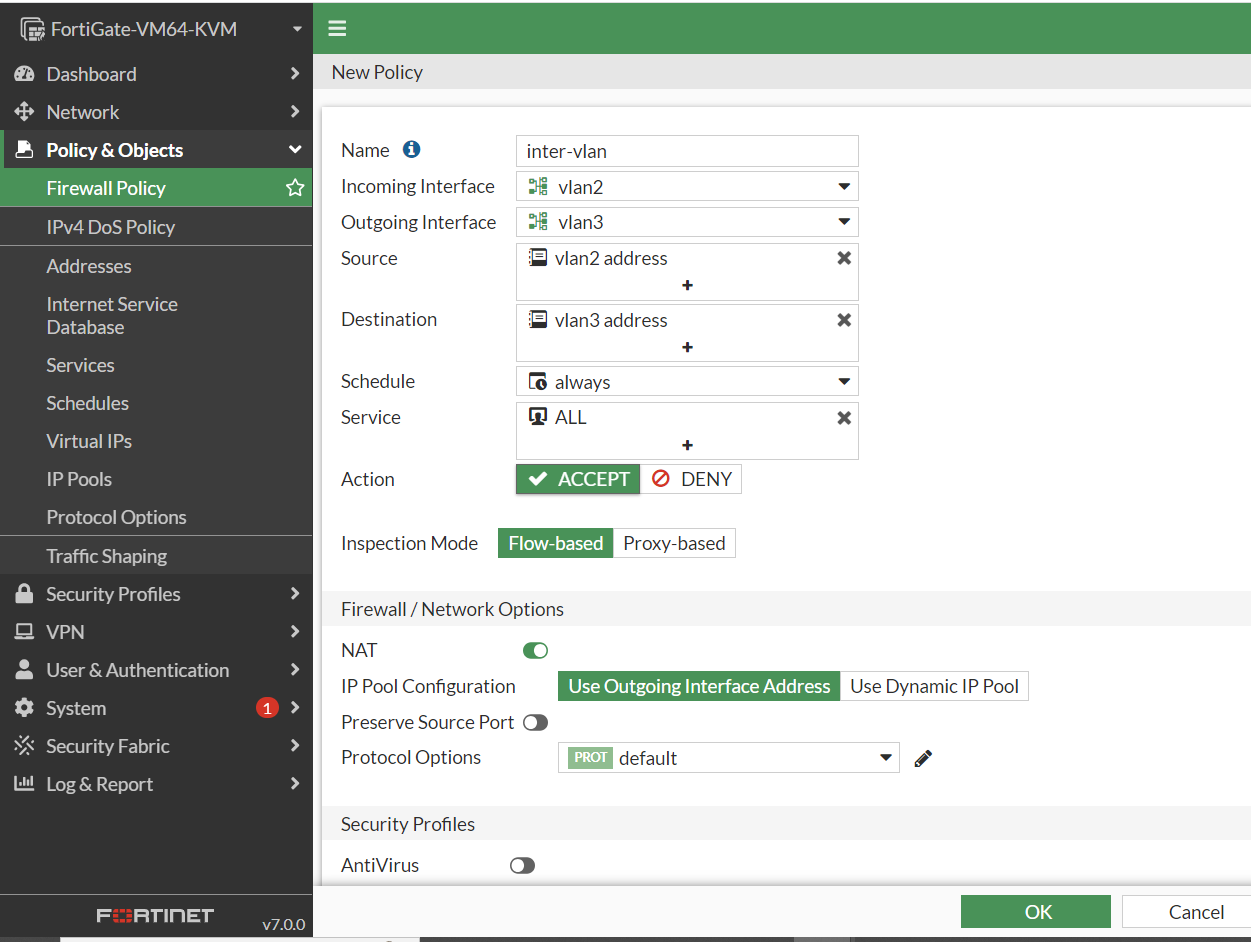
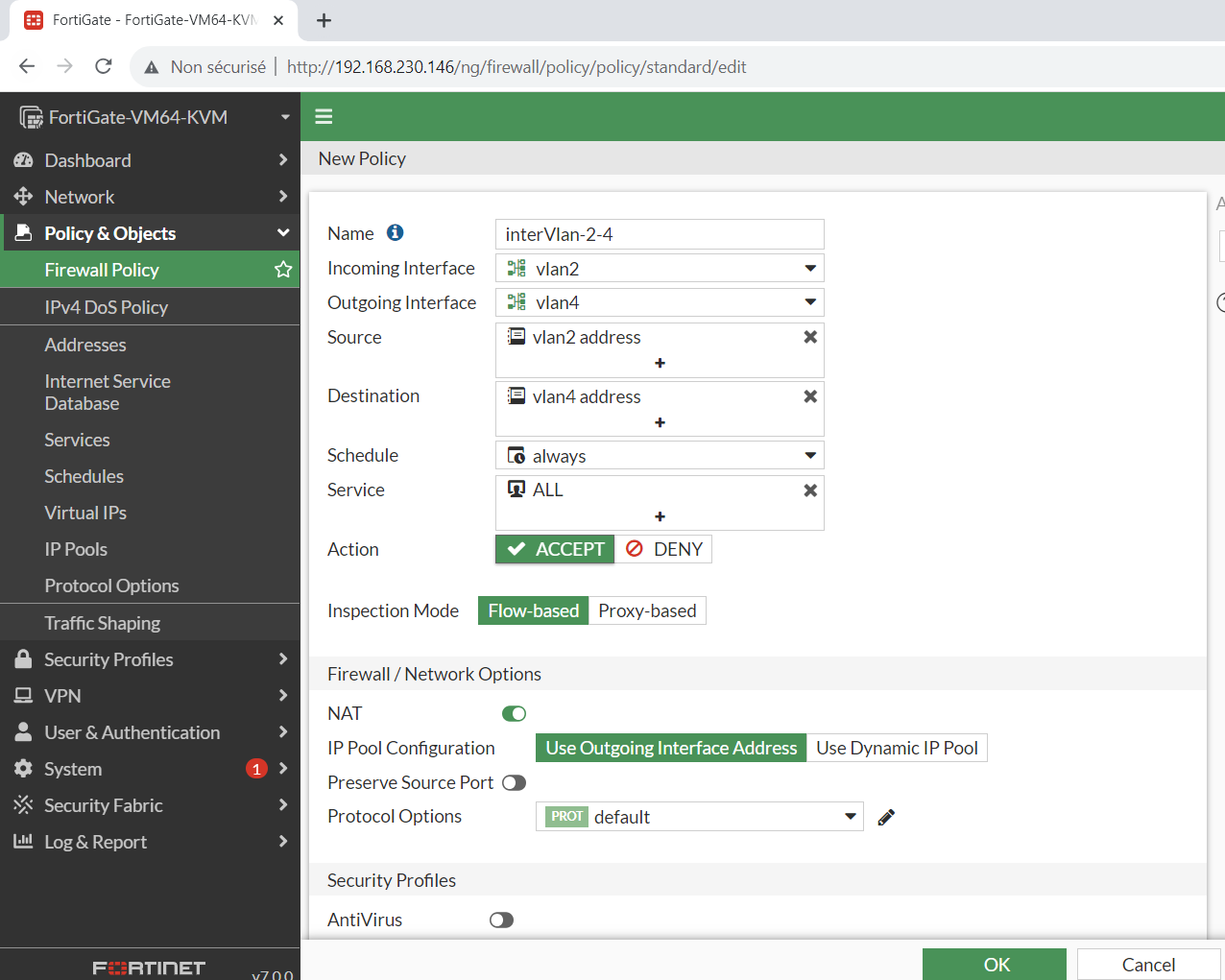
On trouve notre @ IP que DHCP à attribuer dynamiquement avec la commande suivante :

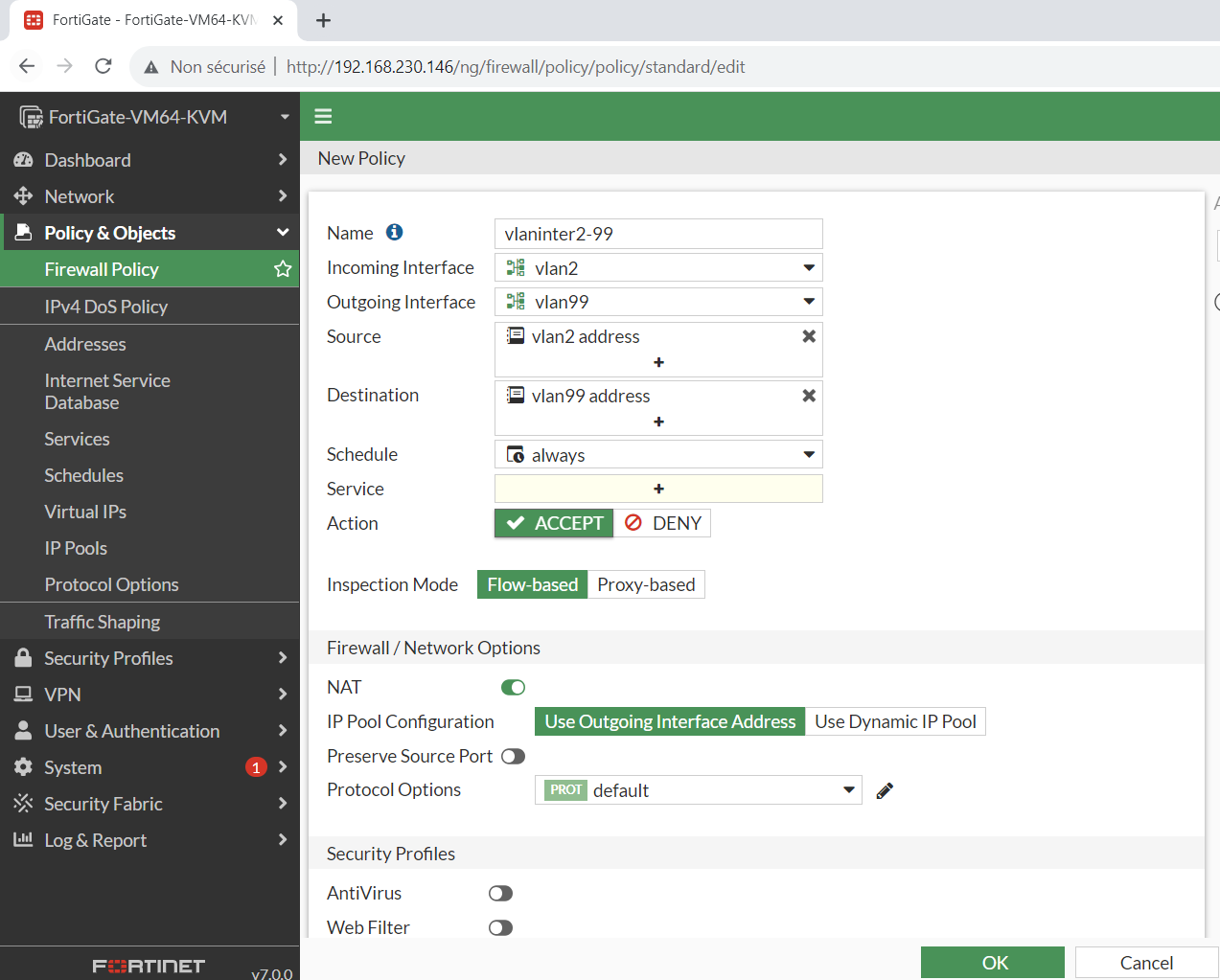
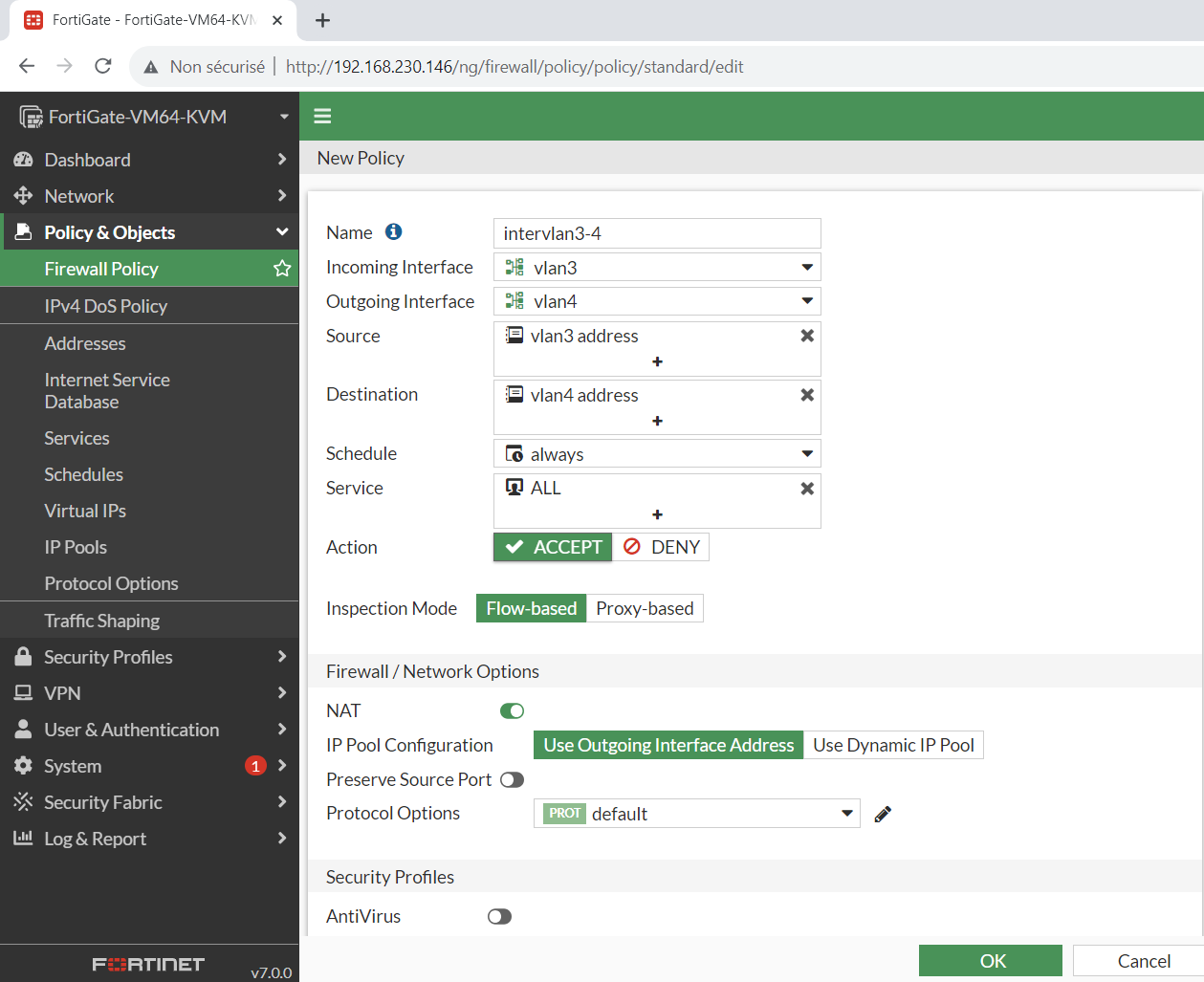


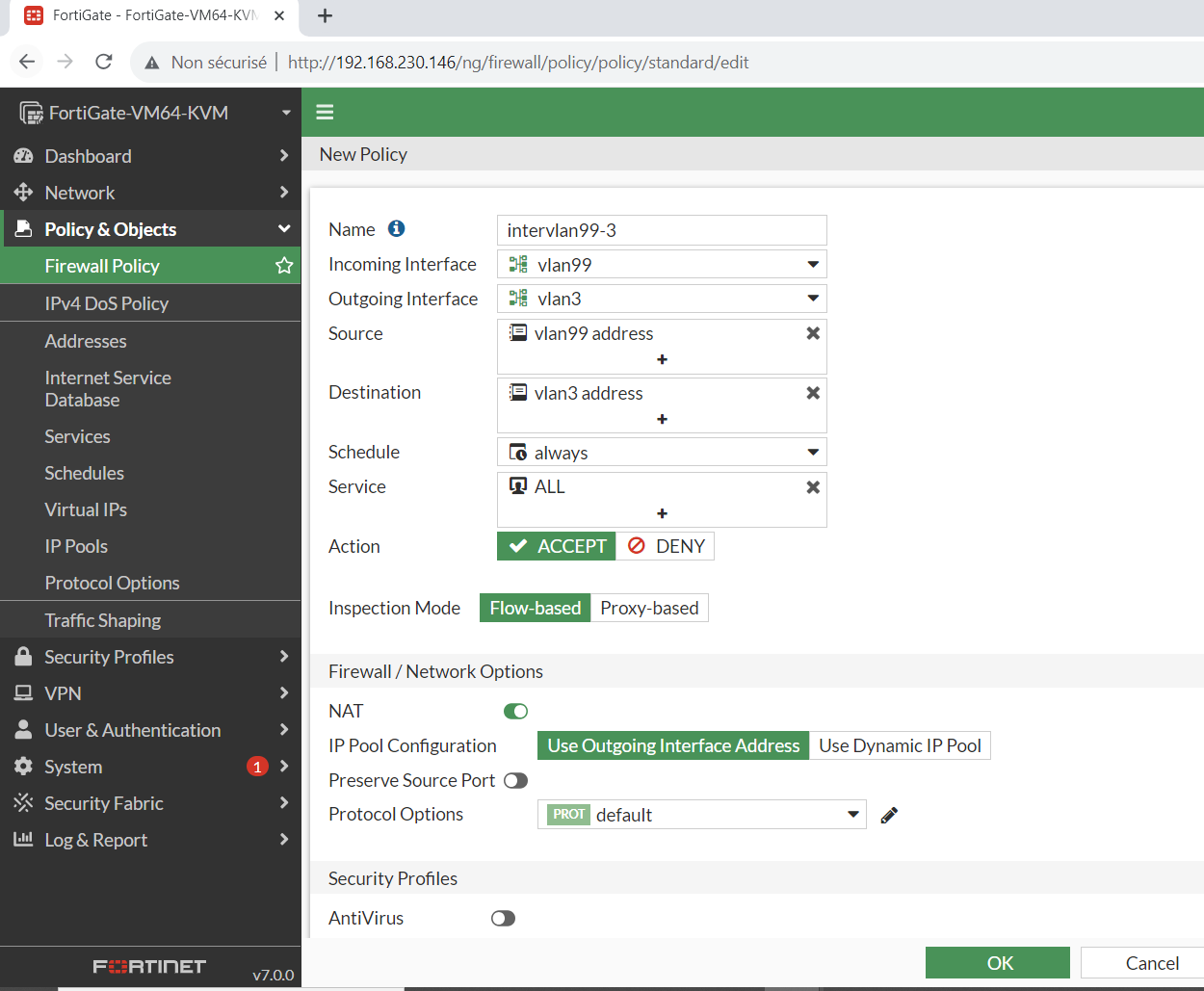
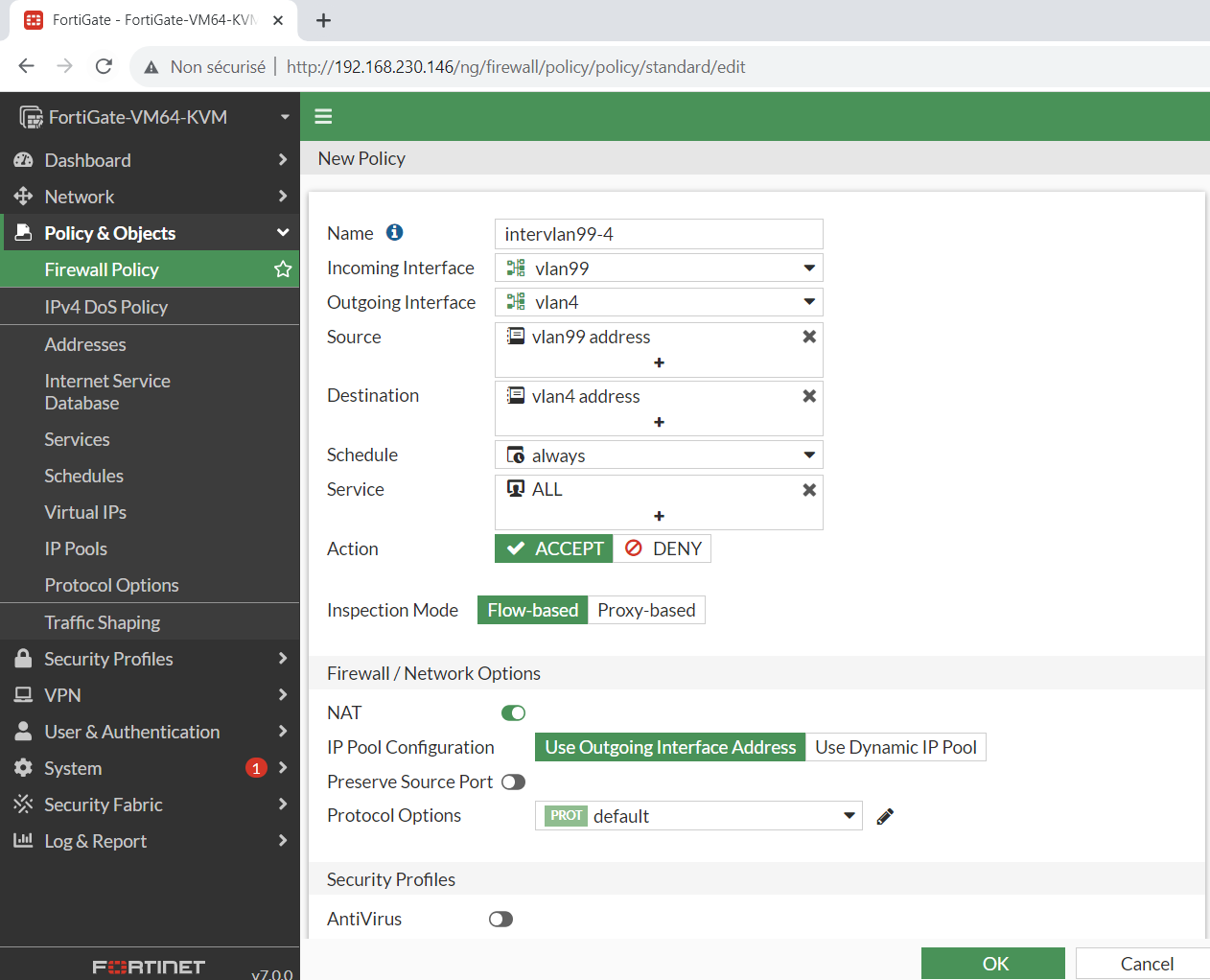
On peut maintenant accéder directement à la version Web de Fortigate en insérant notre@IPduDHCP



7. Activation du routage inter-VLAN dans le FTG

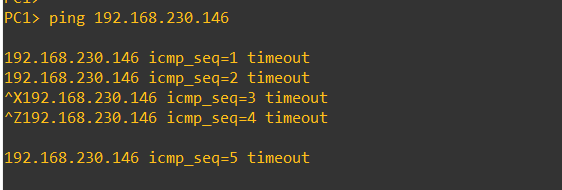
 

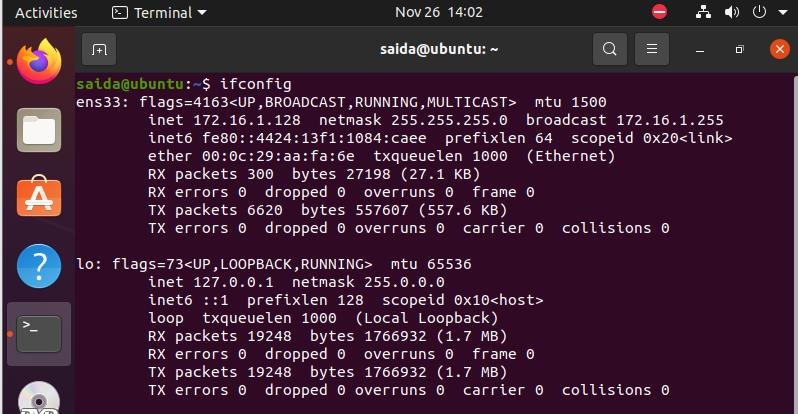
 

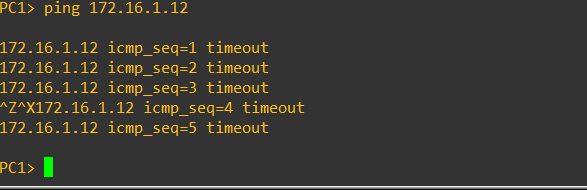
8. **Tester le ping depuis la machine RH vers les passerelles des VLANs de FTG et puis vers vers la machine AG et IT AdminSys**

Ping : RH ---🡪porte 10 de fortigate



Ping : RH🡪 machine AdminSYS





PING: RH 🡪portea de fortigate

