

Sécurité Défensive

Grégoire Roumache

Octobre 2021

Table des matières

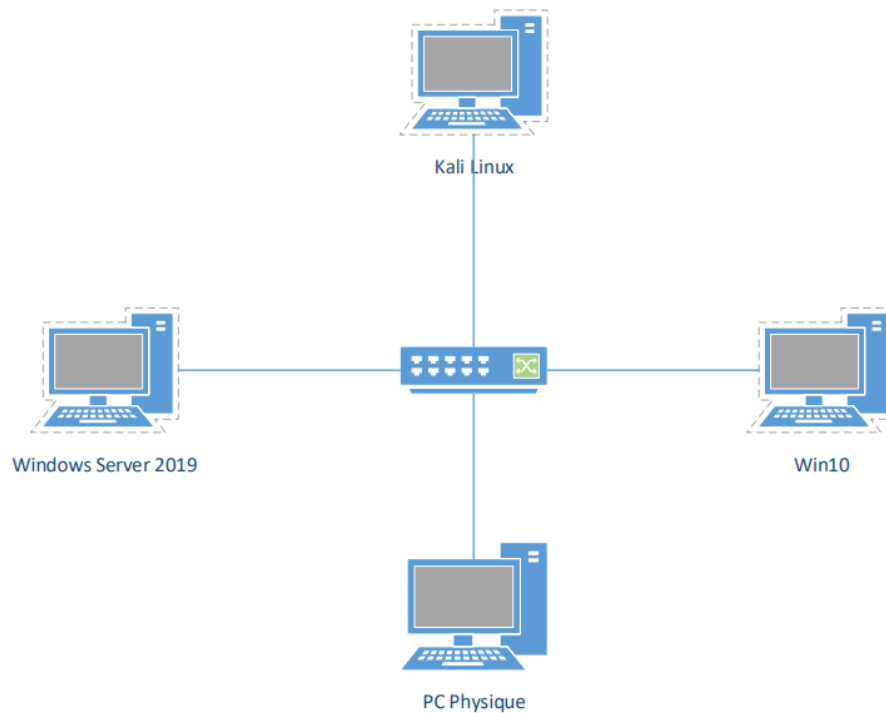
1	Initialiser le switch cisco	1
2	Sécurisation de la couche 2 - port security	2
2.1	Synthèses/notes des années précédentes	2
2.2	Exploration des fonctionnalités du port-security	3
2.3	exercice 3.1 - port-security	3
2.4	DHCP starvation	4
2.5	protection des interfaces autorisant le DHCP	4
3	Sécurisation de la couche 2 - connexion via l'AD/802.1x	5
3.1	Connexion via l'AD - windows server	5
3.2	Connexion via l'AD - switch cisco	7
3.3	Authentification 802.1x - switch cisco	8
3.4	Authentification 802.1x - windows server	9
3.5	Assignation automatique de VLAN	10
3.6	Authentification par certificat	11
4	Palo Alto - Bases	12
4.1	Topologie & Explications sur le labo	12
4.2	Configuration réseau de base	14
4.3	Configuration pour ajouter une machine de la zone client dans l'AD dans la zone serveur	15
5	Palo Alto - UserID (Active Directory)	16
5.1	Configuration de la windows server	16
5.2	Configuration de la Palo Alto	16

1 Initialiser le switch cisco

1. Aller chercher la VM Windows Server 2019 sur le NAS, sur lequel on doit installer le rôle "Network Policy and Access Services" (pas obligé de le faire tout de suite - section 4.1 de l'énoncé). Il faut bien prendre cette VM parce qu'il y a déjà l'AD installé je suppose. Ce qu'on va faire, c'est utiliser un wizard pour y configurer un serveur Radius pour des connections 802.1X.

(<https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-top>)

Remarque: désactiver le parefeu peut nous éviter des problèmes plus tard.



2. Allumer le switch, se connecter au port console du switch avec un **bleu** (le port est potentiellement à l'arrière du switch). Sur l'ordinateur, utiliser putty et le port COM1 ou COM2.
3. Effacer les configurations du switch:
 - (a) `enable`
 - (b) `delete flash:vlan.dat`
 - (c) `erase startup-config`
 - (d) `reload`
4. Configuration de base du switch:
 - (a) `enable`
 - (b) `configure terminal`
 - (c) `line console 0`
 - (d) `logging synchronous`
 - (e) `exit`
 - (f) `write`

2 Sécurisation de la couche 2 - port security

2.1 Synthèses/note des années précédentes

- Méthode de débogage:
<https://github.com/groumache/latex-notes/tree/main/m%C3%A9thode-configuration-packet-tracer>
- Câblage au labo:
<https://github.com/groumache/latex-notes/tree/main/introduction-aux-r%C3%A9seaux-labo-Q2>

2.2 Exploration des fonctionnalités du port-security

1. Connecter le PC physique au switch avec un câble **vert**.
2. Mettre cette interface en mode access et shutdown toutes les autres interfaces (objectif = empêcher les trunks).
 - (a) `interface range f0/1-24`
 - (b) `switchport mode access`
 - (c) `switchport nonegotiate`
 - (d) `interface range f0/2-24` (ici, il faut mettre le bon range !)
 - (e) `shutdown`
3. Activer le mode *debug port-security* pour avoir plus d'infos: `debug port-security`.
4. Activer le switchport *port-security* avec ses options par défaut sur cette interface.
 - (a) `interface <interface>` (interface = f0/1)
 - (b) `switchport port-security`
5. Observer les informations affichées avec les commandes suivantes:
 - (a) `show port-security address`
 - (b) `show port-security interface <interface>`

Sur base de ces informations, que risque-t-il d'arriver si vous connectez une machine virtuelle en pont sur cette même interface ? Faites le test.

Le *violation mode* est *shutdown*, ça signifie que si on connecte une machine virtuelle en pont sur ce même port, l'interface va s'éteindre.

Pour rétablir une interface verrouillée, vous devez commencer par corriger le problème pour ensuite, couper et rétablir l'interface (shutdown => no shutdown sur l'interface).

2.3 exercice 3.1 - port-security

1. Configurer l'interface du switch pour qu'il permette au maximum à 4 adresses MAC de communiquer sur une interface. Ces adresses MAC doivent être sauvegardées dans la running-configuration du switch.
 - (a) `interface <interface>`
 - (b) `switchport port-security maximum <nb>`
 - (c) `switchport port-security mac-address [sticky]`
2. Lorsqu'une infraction est repérée sur une interface, le switch peut réagir de 3 façons différentes (switchport port-security violation {protect | restrict | shutdown}). Recherchez la différence entre ces 3 modes.

	bloque le trafic	message syslog	++ compteur de violation	port shutdown
protect	oui	non	non	non
restrict	oui	oui	oui	non
shutdown	oui	oui	oui	oui

Commande: `switchport port-security violation {protect | restrict | shutdown}`.

3. Pour plus de sécurité, vous pourriez également entrer manuellement les seules adresses MAC autorisées à communiquer sur chaque interface.
 - statique: `switchport port-security mac-address <mac_address>`

- dynamique + statique: `switchport port-security mac-address sticky <mac_address>`
4. Dans un milieu où les utilisateurs changent d'interface de connexion régulièrement, vous pourriez utiliser les options présentes dans: `switchport port-security aging` pour gérer ces utilisateurs.
 - `[static]`: enable aging for configured secure address
 - `[time <1-1440>]`: port security aging time in minutes
 - `[type {absolute|inactivity}]`: port security aging type (default = absolute, inactivity = based on inactivity time period)
 5. Selon vous, quel type d'attaque êtes-vous capable de contrer grâce à cette protection ?
 - DHCP starvation.
 6. Vérification: `show port-security`. Ensuite, enregistrer la configuration avec: `write` (ou: `do write`).

2.4 DHCP starvation

1. Connecter la kali au switch (câble **vert**) et vérifier qu'elle est connectée **uniquement** au switch (en regardant les interfaces et en essayant de ping je suppose).
2. Revérifier que la kali n'est connectée qu'au switch (le prof insiste, peut-être lui demander quoi ?).
3. Configurer un serveur DHCP sur la machine Windows Server.
 - ip **statique** du serveur = 192.168.1.1
 - range d'ip du dhcp = 192.168.1.(10-220)/24
4. Retirer le switchport port-security de l'interface connectée à la machine virtuelle Kali:
 - (a) `interface <interface>`
 - (b) `no shutdown`
 - (c) `no switchport port-security`
5. Avec Kali, lancez une attaque de type DHCP starvation avec le package Yersinia:
 - `sudo yersinia -G dhcp`
6. Observez la distribution des IP sur votre serveur; le pool est épuisé. Essayez d'obtenir une offre DHCP avec un autre client, cela devrait échouer. Après avoir observé ces résultats, refaites la manipulation en activant les options de sécurité adéquates sur le switch pour vous protéger de cette attaque (= activer le port-security, limiter le nombre de mac address, *potentiellement* changer le mode de violation à quelque chose de plus restrictif). Ce type d'attaque est souvent suivi d'une deuxième partie, qui est l'introduction d'un Rogue DHCP server (comme expliqué en cours théorique btw).

2.5 protection des interfaces autorisant le DHCP

1. À l'aide de la commande: `ip dhcp snooping`, préciser quels sont les interfaces sur lesquelles des serveurs DHCP se trouvent, vous protégeant ainsi des rogue DHCP.
 - (a) `interface <interface>`
 - (b) `ip dhcp snooping trust`
 - (c) vérification: `do show ip dhcp snooping | begin pps`

Le DHCP snooping est une fonction de sécurité qui agit comme un pare-feu entre les hôtes non-approuvés et le serveur DHCP approuvé. Fonctionnalités:

- Filtre les messages non-valides.
- Limite le débit du trafic DHCP provenant de sources fiables et non-fiables.

- Gère une base de données DHCP contenant des informations sur les hôtes non-fiables avec des adresses IP louées.
- Utilise cette base de données pour valider les requêtes des hôtes non-fiables.

Remarque: les interfaces sont non-fiables par défaut.

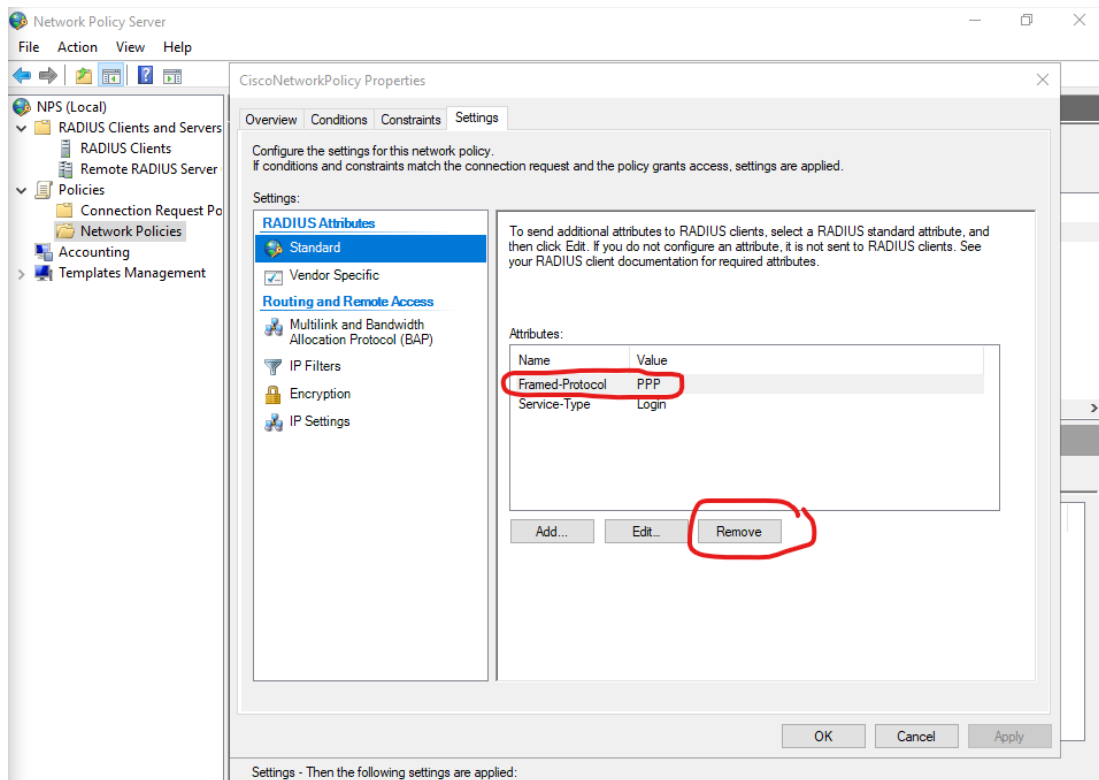
2. Essayez à présent d'empêcher un rogue DHCP (depuis votre Kali par exemple) d'offrir des bails DHCP aux clients connectés au switch. Utilisez une deuxième interface du switch pour vous faciliter la vie.

Si on n'a pas deux machines, on peut mettre le trust sur un autre port et vérifier que le serveur DHCP de la machine windows server n'arrive pas à donner une adresse IP à une VM en pont connecté au switch sur la même interface.

3 Sécurisation de la couche 2 - connexion via l'AD/802.1x

3.1 Connexion via l'AD - windows server

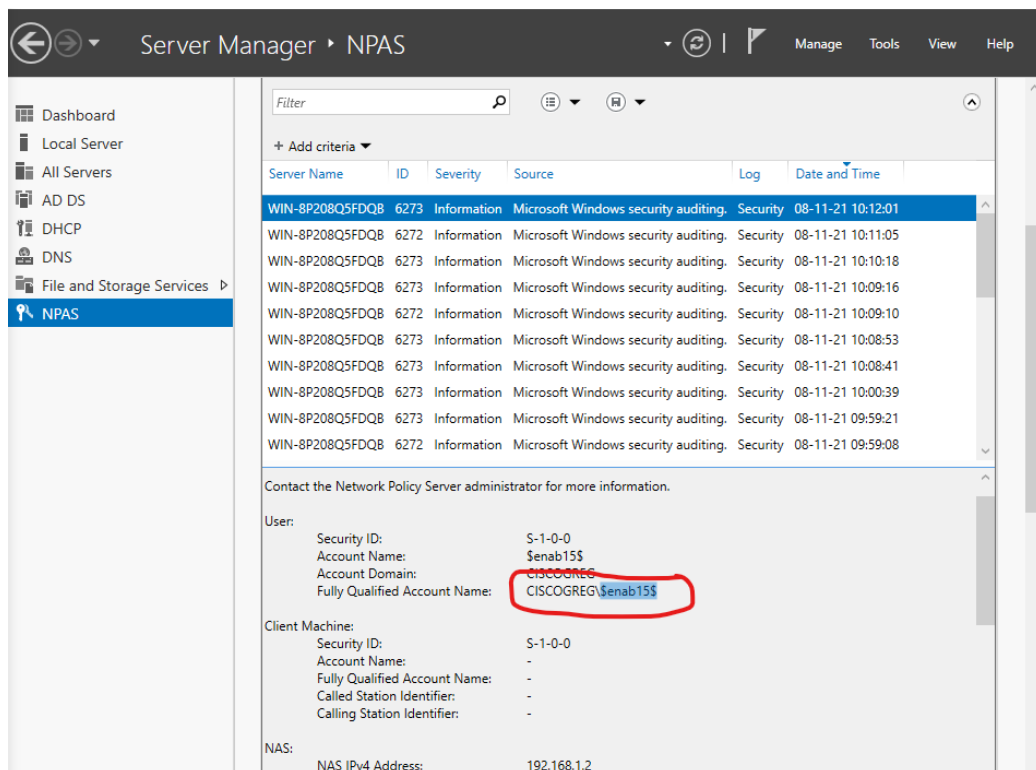
1. Installer et configurer le service AD (Active Directory):
 - (a) ouvrir le *server manager*
 - (b) en haut à droite, cliquer sur *manage*, puis sur *add roles and features*
 - (c) à gauche dans *server roles*, sélectionner *active directory domain services*
 - (d) cliquer sur *add features* dans la popup, puis continuer jusqu'à l'installation
 - (e) quand un signe danger apparaît en haut à droite, cliquer dessus
 - (f) cliquer sur *promote this server to a domain controller*
 - (g) sélectionner l'option *add a new forest*, et ajouter le nom de domaine (ex: *ciscogreg.local*)
 - (h) ensuite, ajouter le mot de passe DSRM: *Tigrou007*, et terminer la configuration
2. Aller dans *active directory users and computers* et ajouter:
 - un groupe `cisco_admin` à l'AD
 - ajouter un utilisateur `admin1` dedans
3. Installer le service NPS (Network Policy Server) et ajouter le switch en tant que client radius:
 - (a) clic droit sur *RADIUS Clients and Servers/RADIUS Clients*, puis cliquer sur *New*
 - (b) ajouter un "friendly name" comme *SwitchCisco*, l'IP du switch et un secret partagé comme *Tigrou007*
4. Ajouter une politique de connexion au service NPS:
 - dans NPS, clic droit sur *nps/policies/network policies* et cliquer sur *new*
 - dans *policy name*, mettre *CiscoSwitchManagement*, puis cliquer sur *next*
 - ajouter une condition telle que seul le groupe windows `CISCOGREG\cisco_admin` soit concerné par la règle, puis cliquer sur *next*
 - ajouter la méthode d'authentification non-chiffrée *PAP, SPAP*
 - une fois arrivé dans *configure constraints*, aller dans le sous-menu *NAS Port Type*
 - sélectionner *async (modem)* et *virtual (vpn)*, puis cliquer sur *next*
 - supprimer l'attribut *Framed-Protocol* de valeur *PPP*



5. Configuration pour pouvoir se connecter en mode **enable**:

- créer l'utilisateur **\$enab15\$** dans l'AD
- l'ajouter au groupe **cisco_admin**

On fait ainsi parce que quand on essaie de passer en mode **enable**, le switch tente de se connecter avec cet utilisateur.



6. Si ce n'est toujours pas fait, désactiver le parefeu windows.

3.2 Connexion via l'AD - switch cisco

1. Configurer l'interface VLAN1:

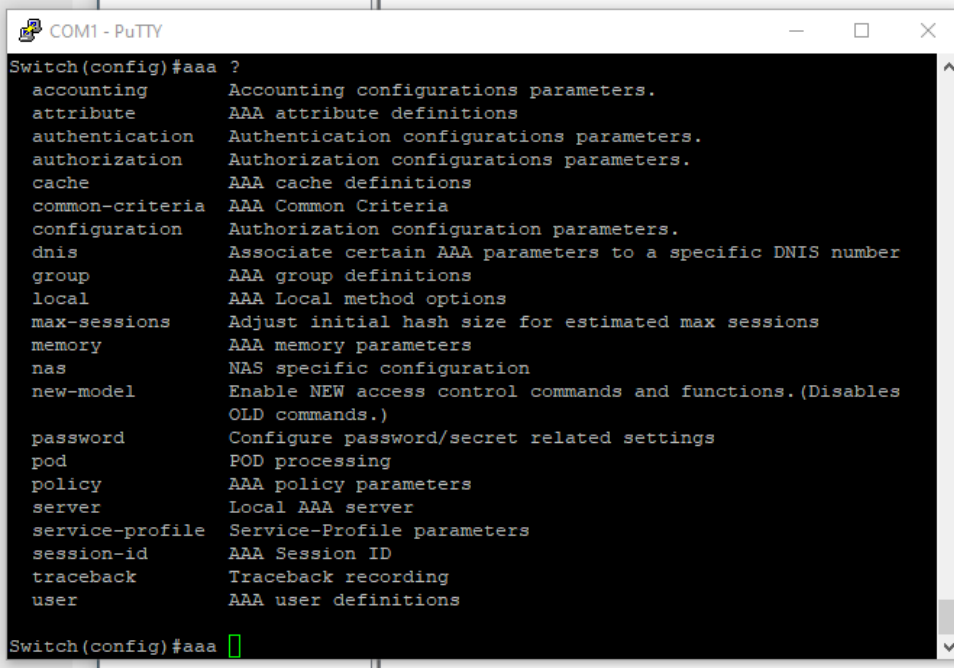
- `interface vlan1`
- `no shutdown`
- `ip address 192.168.1.2 255.255.255.0`

2. Activer SSH:

- `line vty 0 15`
- `transport input ssh`
- ajouter le domaine de l'AD: `ip domain-name <domain>` (ip domain-name ciscogreg.local)
- ajouter un compte local pour se connecter au cas où: `username greg privilege 1 secret Tigrou007`
- `exit`
- `crypto key generate rsa`

3. Quelles sont les sous-commandes de `aaa` ?

- (a) `aaa new-model`
- (b) `aaa` ?



```
Switch(config)#aaa ?
accounting      Accounting configurations parameters.
attribute       AAA attribute definitions
authentication   Authentication configurations parameters.
authorization    Authorization configurations parameters.
cache           AAA cache definitions
common-criteria AAA Common Criteria
configuration    Authorization configuration parameters.
dnis            Associate certain AAA parameters to a specific DNIS number
group           AAA group definitions
local           AAA Local method options
max-sessions     Adjust initial hash size for estimated max sessions
memory          AAA memory parameters
nas            NAS specific configuration
new-model       Enable NEW access control commands and functions. (Disables
                OLD commands.)
password        Configure password/secret related settings
pod            POD processing
policy          AAA policy parameters
server          Local AAA server
service-profile Service-Profile parameters
session-id      AAA Session ID
traceback       Traceback recording
user           AAA user definitions

Switch(config)#aaa
```

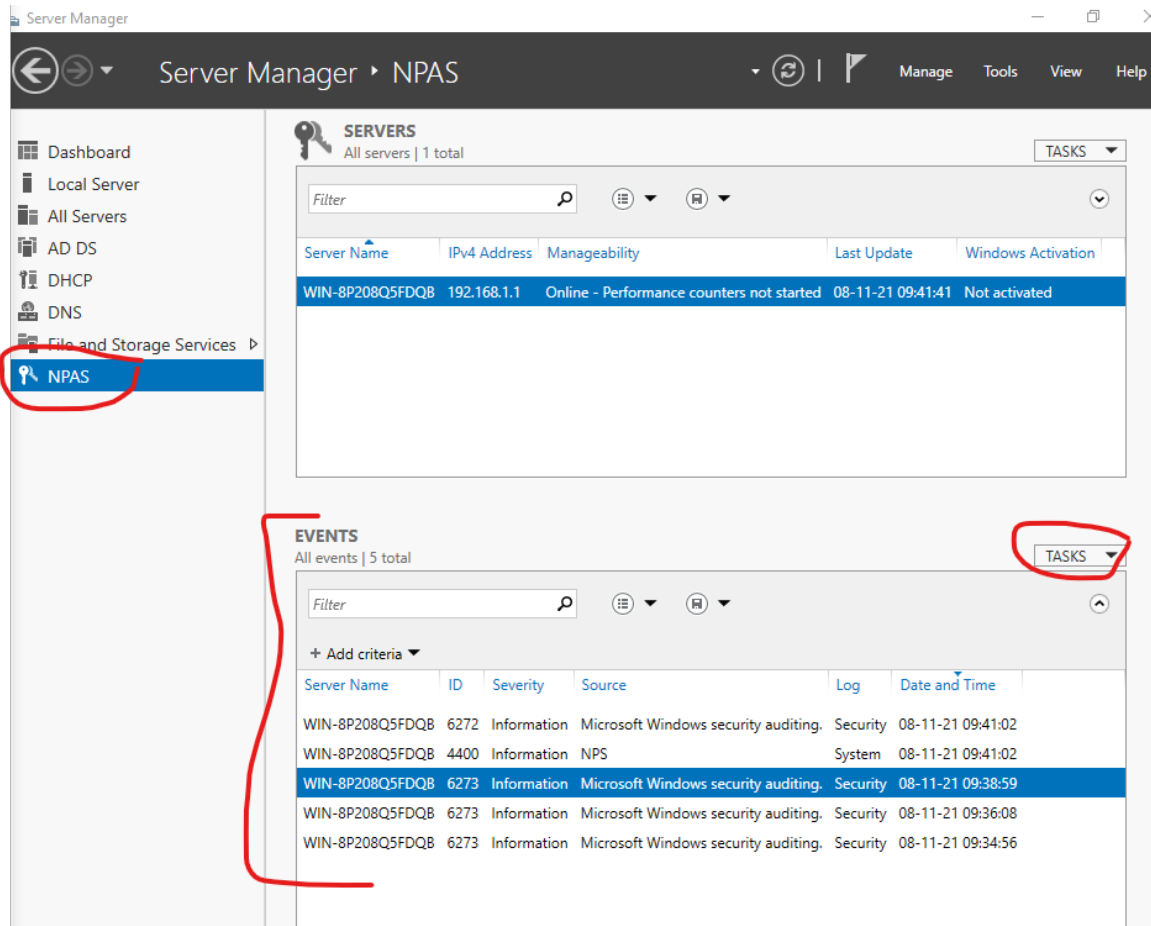
4. Activer l'authentification avec le serveur radius:

- (a) informations du serveur radius: `radius server host <server_ip> key <shared_secret>`
- (b) autoriser l'authentification par mdp: `aaa authentication login default group radius enable`
- (c) autoriser l'authentification par radius: `aaa authentication enable default group radius enable`
- (d) donner les permissions enable aux utilisateurs connectés via radius: `aaa authorization exec default group radius if-authenticated`

Essayez de vous connecter en SSH sur le switch. Utilisez le mot de passe de l'utilisateur \$enab15\$ pour passer en mode enable.

5. En cas de problème, on peut consulter les logs du rôle Network Policy and Access Service (NPAS).

Pour vérifier, on peut faire *exit* pour se déconnecter (pas besoin de débrancher/rebrancher le câble bleu) et se reconnecter. Si il y a des problèmes, on peut se connecter en SSH avec le compte local et reconfigurer.



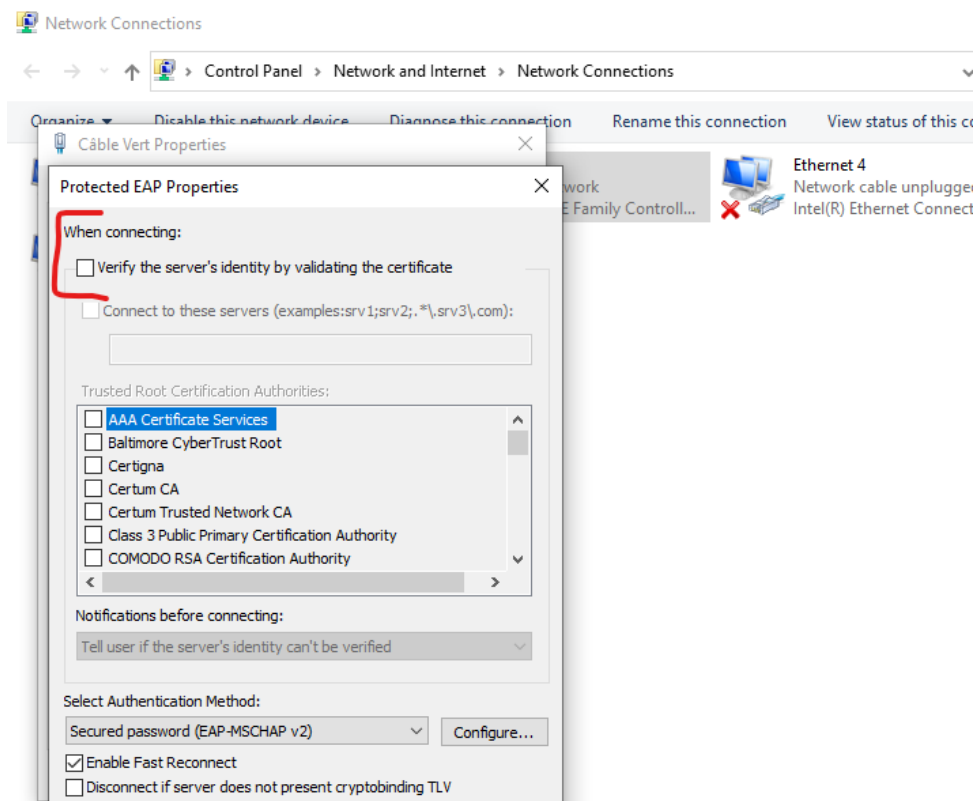
3.3 Authentification 802.1x - switch cisco

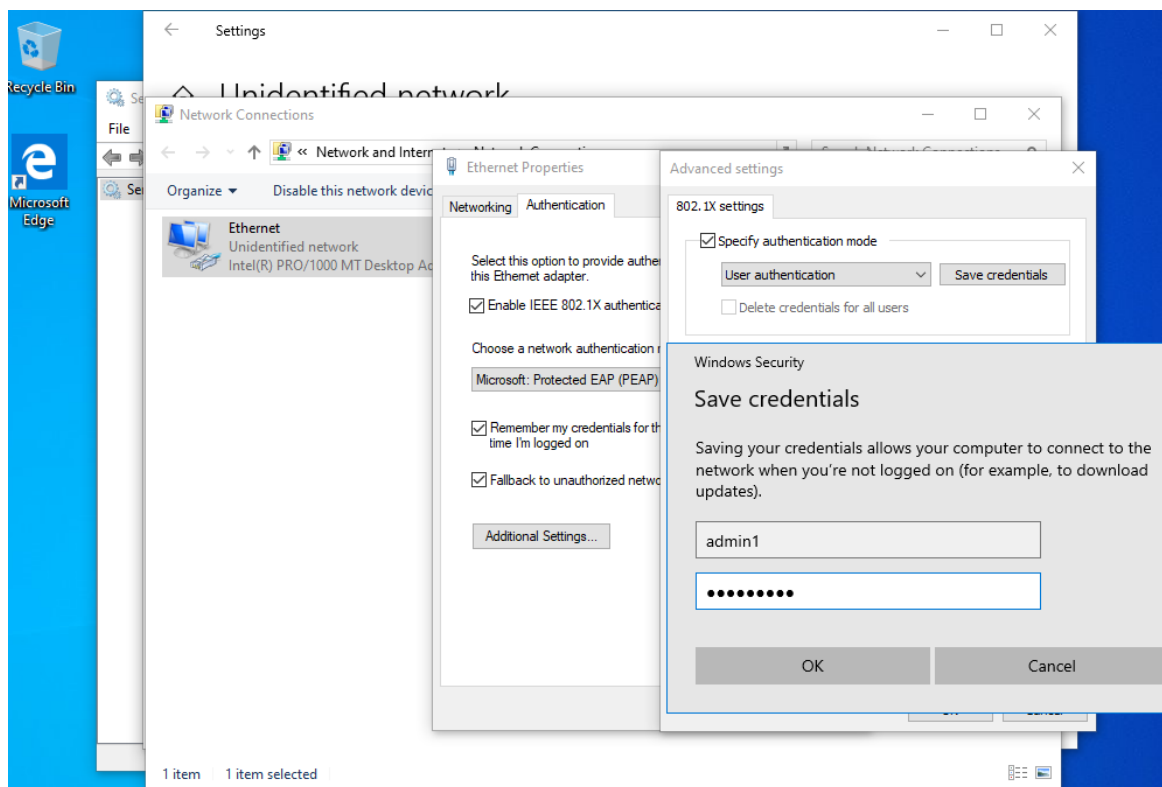
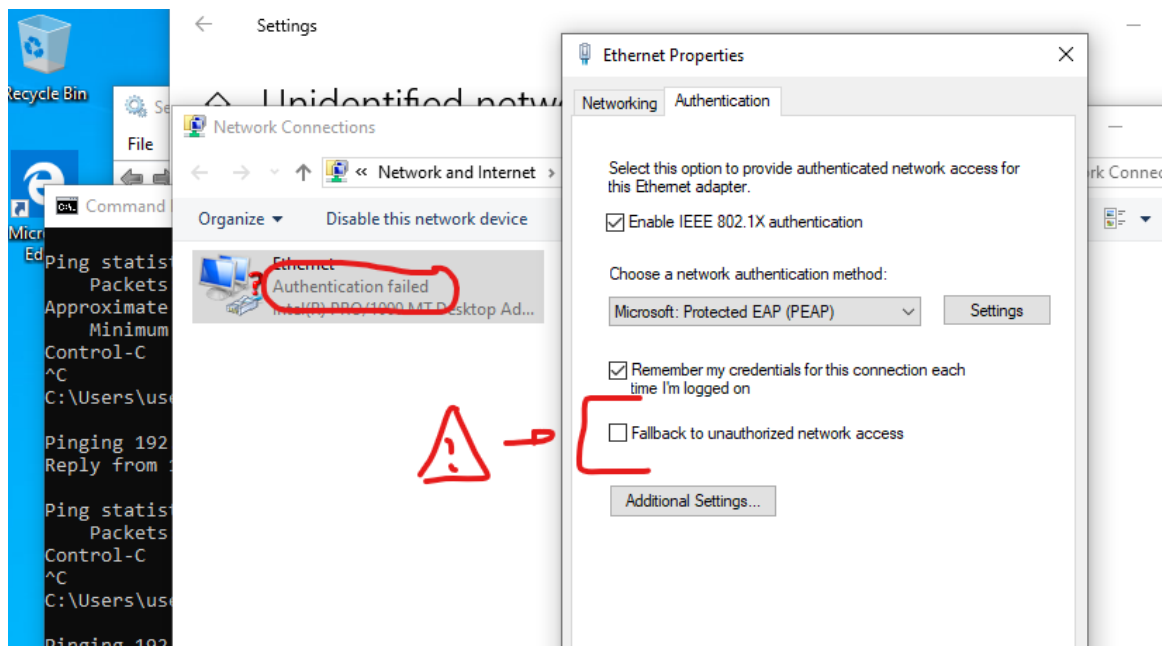
1. Configurer l'authentification des machines se connectant à une des interfaces en dot1x:
 - (a) `dot1 system-auth-control`
 - (b) `aaa authorization network default group radius if-authenticated`
 - (c) `aaa authentication dot1x default group radius`
2. Sur l'interface du switch où vous voulez configurer le 802.1x:

vieux switch	nouveau switch
(a) <code>switchport mode access</code> (b) <code>dot1x port-control auto</code> (c) <code>debug dot1x all</code>	(a) <code>switchport mode access</code> (b) <code>authentication port-control auto</code> (c) <code>dot1x pae authenticator</code> (d) <code>debug dot1x all</code>

3.4 Authentication 802.1x - windows server

1. Installer le rôle ADCS (Active Directory Certificate Service) sur la windows server. Il faut créer une CA (certificate authority) mais pas besoin de créer un certificat.
2. Se connecter au switch (avec le câble vert) avec un mot de passe:
 - (a) lancer: `services.msc`
 - (b) démarrer le service: `wired autoconfig`
 - (c) aller dans `ncpa.cpl` et suivre les captures d'écrans suivantes





3.5 Assignment automatique de VLAN

Objectif = changer automatiquement le VLAN du port en fonction du groupe auquel l'utilisateur connecté appartient.

1. Sur le switch, créer les 3 vlans:

- `vlan <number>`
- `name <name>`

2. Sur le serveur, aller dans l'*active directory users and computers* et créer les 3 groupes (ex: *vlan10*) et 3 utilisateurs (ex: *user-vlan10*) pour chaque groupe.
3. Installer le service DHCP et créer 3 réseaux, 1 pour chaque vlan:
 - (a) dans la fenêtre de gestion du DHCP, faire un clic droit sur *<server>.ciscogreg.local/ipv4*
 - (b) cliquer sur *new scope*, dans *name* entrer *vlan10*
 - (c) entrer le range d'ip suivant: *192.168.10.10 - 192.168.10.250*
 - (d) pas besoin d'entrer une default gateway vu qu'on n'a pas de routeur
4. Ouvrir *Network Policy Server*
 - (a) aller dans *Policies/Network Policies*
 - (b) créer une nouvelle policy *CiscoVlan10*
 - (c) ajouter le groupe windows *vlan10*
 - (d) ajouter la méthode d'authentification *PAP, SPAP*
 - (e) dans *nas port type*, ajouter *async (modem)* et *virtual (vpn)*
 - (f) retirer l'attribut *Framed-Protocol* de valeur *PPP*
 - (g) ajouter les attributs suivants (access type = 802.1x):

Attribut	Valeur
Tunnel-Type	802.1x - Virtual LANs (VLAN)
Tunnel-Medium-Type	802.1x - 802 (includes all 802 media ...)
Tunnel-Pvt-Group-ID	10 (10 = numéro du vlan)

5. Sur la windows client (qui se connecte avec le câble vert au switch), démarrer le service *WLAN AutoConfig* dans *services.msc*.

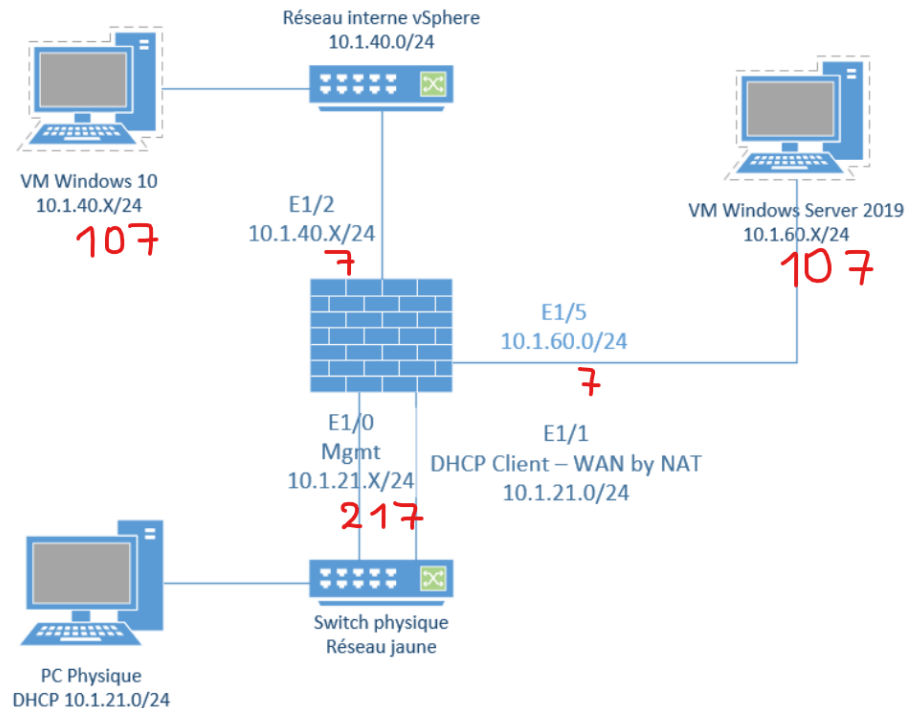
3.6 Authentification par certificat

Pas à l'examen.

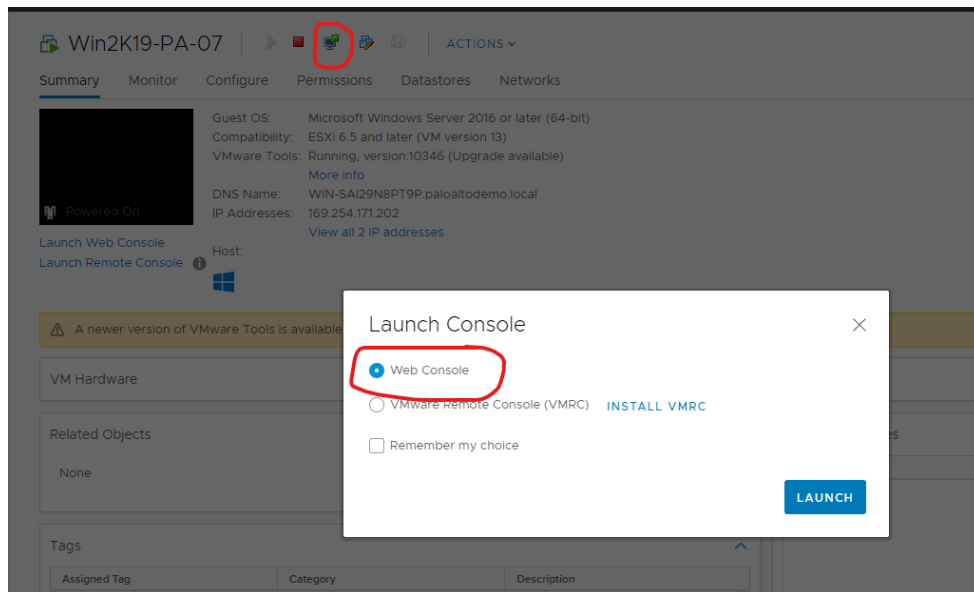
4 Palo Alto - Bases

4.1 Topologie & Explications sur le labo

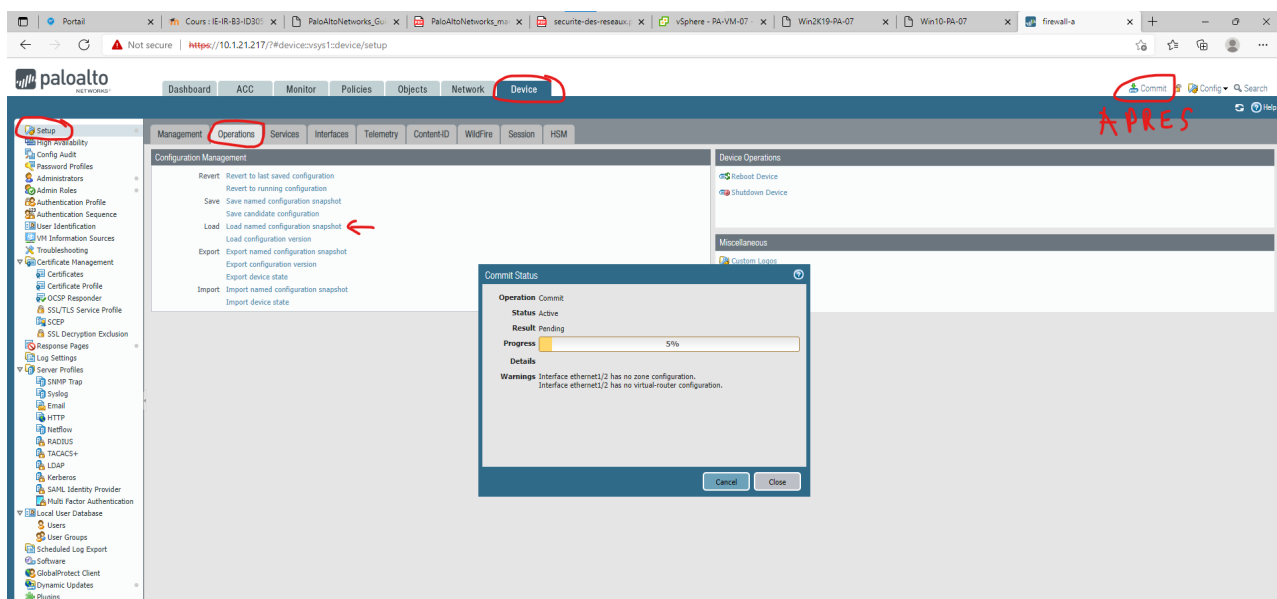
- Topologie:



- L'interface 0 (l'interface de management) est déjà configurée, on y accède via l'interface web, pas besoin de faire des changements.
- Une fois qu'on a configuré le parefeu pour que les machines puissent se ping et accéder à internet, il faudra suivre le chapitre User-ID de palo alto (l'user-id agent est sur moodle).
- L'objectif final est de pouvoir vérifier l'identité/les accès àpd utilisateurs de l'AD.
- Pour se connecter à vsphere, il faut utiliser ces identifiants: **Student@vsphere.local** - **Tigrou007=**, à l'adresse: **https://10.1.31.191/**.
- Pour se connecter à l'interface web de palo alto, il faut aller sur: **https://<ip>/** (dans mon cas: **https://10.1.21.217/**) et utiliser les identifiants: **admin** - **admin**.
- On peut ouvrir les machines windows, à partir de l'interface vsphere comme ceci:



- Enfin, il faut charger une configuration vide dans palo alto comme ceci:



4.2 Configuration réseau de base

1. Créer les 4 zones (zone-client, zone-server, zone-management, zone-wan).

Dans `network/zones`:

- name = zone-client
- type = layer 3

2. Créer des *interface management profile* (pour autoriser le ping et autre).

Dans `network/network profiles/interface mgmt`:

- name = ping-and-response-pages
- network services = ping, response pages

3. Créer un routeur virtuel pour router le trafic entre les interfaces.

Dans `network/virtual routers`:

- name = routeur-virtuel
- interfaces = ethernet1/1, ethernet1/2, ethernet1/5

4. Configurer les interfaces ethernet.

Dans `network/interfaces/ethernet`:

- interface name = ethernet1/1
- comment = server-side
- interface type = layer 3
- virtual router = routeur-virtuel
- security zone = server-side
- ipv4/ip = 10.1.60.7/24 (ne pas mettre d'ip pour les interfaces en dhcp)
- advanced/management profile = ping-and-response-pages

5. Créer 2 politiques de source nat (1 pour la zone client et 1 pour la zone serveurs).

Dans `policies/nat`:

- general/name = nat-client-zone
- original packet/source zone = client-zone
- original packet/destination zone = wan
- original packet/destination interface = ethernet1/1
- translated packet/translation type = dynamic ip and port
- translated packet/address type = interface address
- translated packet/interface = ethernet1/1

6. Créer des politiques de sécurité pour:

- autoriser le trafic vers internet (vers le wan)
- autoriser le trafic entre les zones internes

Dans `policies/security`:

- `general/name` = client-server-to-wan
- `source/zone` = client-zone, server-zone
- `destination/zone` = wan

7. Commit tous les changements et tester la connectivité avec internet et entre les machines.

4.3 Configuration pour ajouter une machine de la zone client dans l'AD dans la zone serveur

1. Modifier la politique de sécurité qui autorise le trafic entre les zones client et serveur.

Dans l'onglet `application`:

- ntp
- dns
- ms-netlogon
- kerberos
- ldap
- msrpc
- active-directory
- netbios-ss
- ms-ds-smb-base
- ms-ds-smbv2
- ms-ds-smbv3
- net.tcp
- netbios-ns
- netbios-dg

2. Sur la windows server contenant l'active directory, trouver le nom de domaine de l'AD.
3. Modifier le DNS de la windows 10 (il faut que ce soit l'ip de la windows server).
4. Ajouter la windows 10 à l'AD.

Ouvrir le *control panel* sur la windows 10,

- (a) aller dans *system and security*, puis dans *system*
- (b) à droite, cliquer sur *change settings*, puis sur le bouton *change*
- (c) sélectionner le bouton radio *domain*
- (d) entrer le nom du domaine (ici, *paloaltdemo.local*), puis appuyer sur *ok*
- (e) se connecter avec un compte de l'AD (ici, *Administrator - Tigrou007=*)

5 Palo Alto - UserID (Active Directory)

5.1 Configuration de la windows server

1. ouvrir *active directory users and computers* et créer un compte dans le domaine sous *managed service accounts* (ex: *greg-user-id*)
2. toujours dans *managed service accounts*, créer un groupe (ex: *group-user-id*) et y ajouter l'utilisateur créé
3. ouvrir *local security policy* (avec: *gpedit.msc*) et aller dans *local policies/user rights assignment/log on as a service* et ajouter l'utilisateur créé (ex: *<domaine>\greg-user-id*)
4. ouvrir *group policy management* (avec: *gpmc.msc*) et modifier la *default domain policy*
5. dans la fenêtre *group policy management editor*, modifier la règle *computer configuration/policies/windows settings/security settings/local policies/user rights assignments/log on as a service* et ajouter l'utilisateur créé (ex: *<domaine>\greg-user-id*)
6. télécharger *paloalto-useragent-install.msi* qui se trouve dans le nas
 - `\\10.1.21.204\TI-Student\IR305`
 - Student - Tigrou007
7. installer l'agent user-id et aller dans *C:\Program Files (x86)\Palo Alto Networks*
 - faire un clic droit sur le dossier *User-ID Agent* et aller dans *propriétés*
 - aller dans l'onglet *security*, cliquer sur *edit*
 - mettre comme owner l'utilisateur créé (ex: *<domaine>\greg-user-id*) et lui donner toutes les permissions
8. ouvrir *user-id agent* et aller dans *user identification/discovery*
 - (a) ajouter un serveur:
 - name = server-user-id
 - server address = *<ip-pao-alto>*
 - server type = microsoft active directory
 - (b) ajouter 2 configurations réseau (1 pour le réseau client, 1 pour le réseau serveur):
 - names = server-network-user-id, client-network-server-id
 - network address = 10.1.60.0/24, 10.1.40.0/24
9. aller dans *user identification/setup*, cliquer sur *edit*, aller dans l'onglet *client probing*, décocher les cases
10. désactiver le parefeu de la windows server

5.2 Configuration de la Palo Alto

1. Activer l'User Identification (= User-ID):
 - Dans *network/zones*:
 - éditer la zone client
 - cocher la case *enable user identification*
2. Ajouter un profil serveur LDAP:

Dans `device/server profiles/ldap`:

- profile name = ldap-server-profile
- server list/name = ldap-server
- server list/ldap server = <ip-windows-server>
- server list/port = 389
- type = active-directory
- base dn = DC=paloaltodemo,DC=local
- bind dn = CN=Administrator,CN=Users,DC=paloaltodemo,DC=local
- password = <mdp-admin-domaine>
- décocher la case *require ssl/tls secured connection*

3. Ajouter une configuration de group-mapping:

Dans `device/user identification/group mapping settings`:

- name = group-mapping-user-id
- server profile = ldap-server-profile
- group include list = ajouter le groupe d'utilisateurs autorisé

4. Ajouter une configuration de user-mapping (`device/user identification/user mapping`).

5. Ajouter un user-id agent:

Dans `device/user identification/user-id agents`:

- name = agent-user-id
- host = <ip-windows-server>
- port = 5007
- enabled = coché

6. Modifier les configurations de routes de services:

Dans `device/setup/services`, cliquer sur `service route configuration`:

- sélectionner *customize*
- ldap, uid agent:
 - source interface = <interface-windows-server>
 - source address = <ip-sur-interface-windows-server>

7. Modifier la règle de sécurité d'accès à internet pour la restreindre aux utilisateurs de l'AD:

Dans `policies/security`, modifier la règle d'accès à internet pour les clients:

- user/source user = paloaltodemo\group-user-id
- user/source user = paloaltodemo\greg-user-id
- user/source user = paloaltodemo\Administrator

8. Vérifier que tout fonctionne en se connectant en admin du domaine ou avec le compte service (`greg-user-id`) sur la windows 10 et essayer d'accéder à internet.