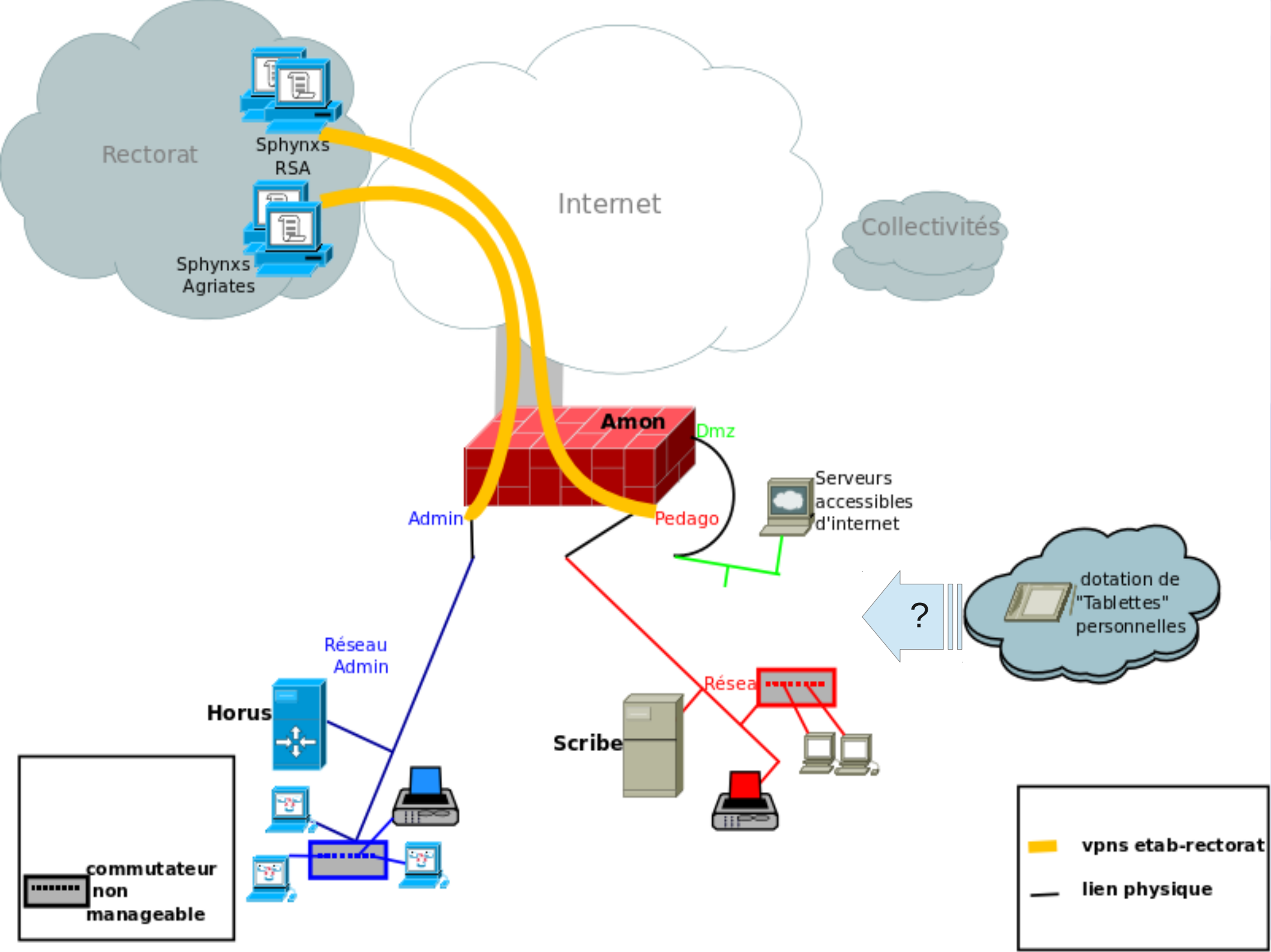
J-Eole 2013

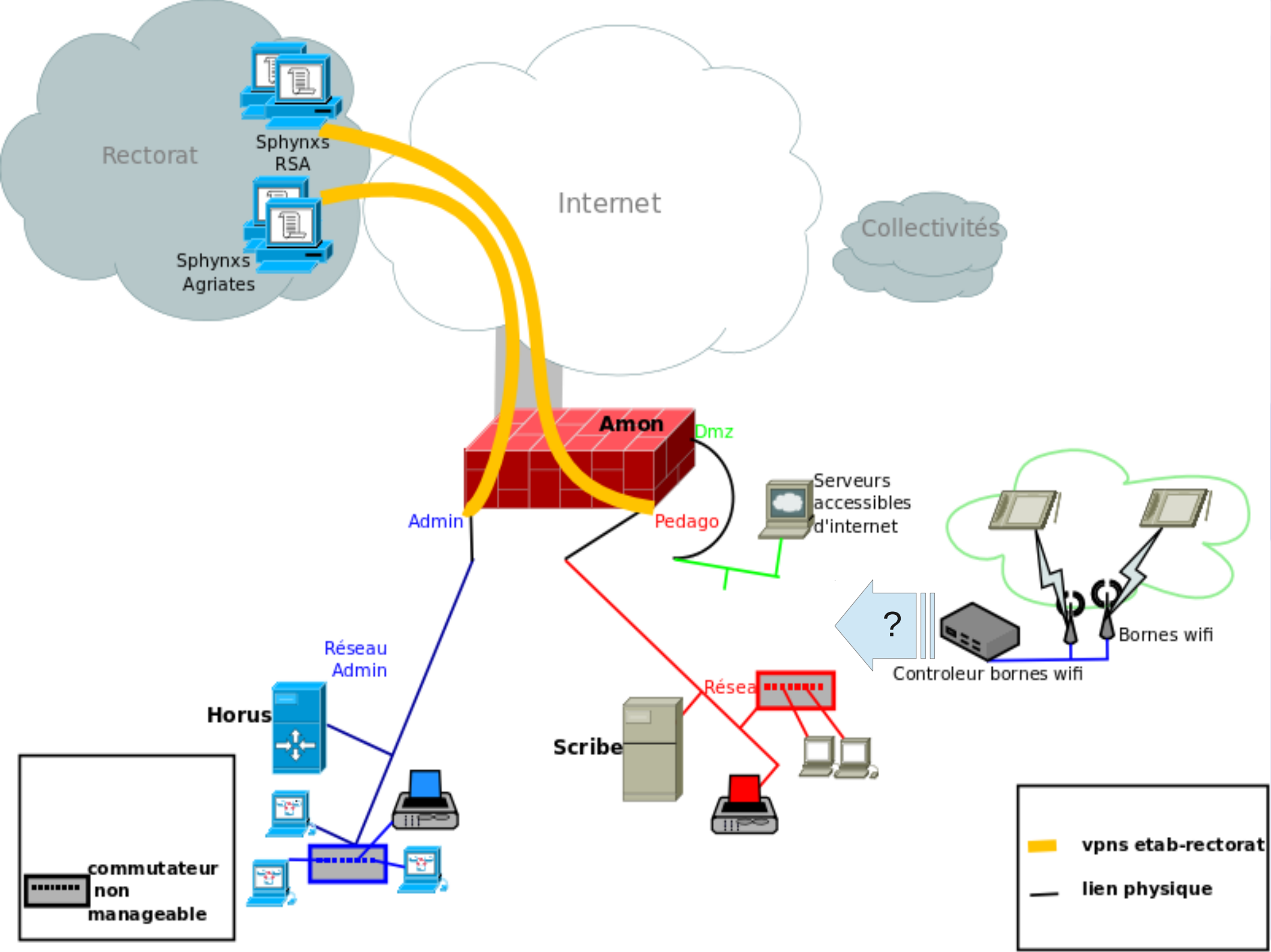
Utilisation de freeradius sur Amon dans le cadre d'un usage Wifi en établissement scolaire

- Dotation de tablettes personnelles à l'ensemble des collégiens du département (tous les 6èmes tous les ans)
- Couverture Wifi globale des 26 établissements.
  - 600 bornes
- Restructuration totale des réseaux internes des collèges :
  - infrastructures en étoile,
  - câblage cat 6A (6500 prises rj45),
  - harmonisation des actifs (170 commutateurs HP marché UGAP)

Obligations et objectifs

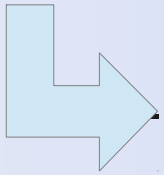
- Sécuriser l'accès au Wifi
- Respecter la loi :
  - filtrage des accès Internet depuis les tablettes
  - historisation nominative des accès depuis les tablettes (un an)
- Faciliter la gestion, la supervision


Rectorat
Sphynxs
RSA
Sphynxs
Agriates
Internet
Collectivités
Amon
Dmz
Admin
Pedago
Serveurs
accessibles
d'internet
?
dotation de
"Tablettes"
personnelles
Réseau
Admin
Horus
Scribe
Réseau
commutateur
non
manageable
vpns etab-rectorat
lien physique

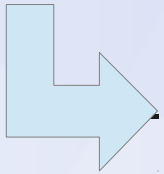

Rectorat
Sphynxs
RSA
Sphynxs
Agriates
Internet
Collectivités
Amon
Dmz
Admin
Pedago
Serveurs
accessibles
d'internet
?
Bornes wifi
Controleur bornes wifi
Réseau
Admin
Horus
Scribe
Réseau
commutateur
non
manageable
vpns etab-rectorat
lien physique

Evolutions

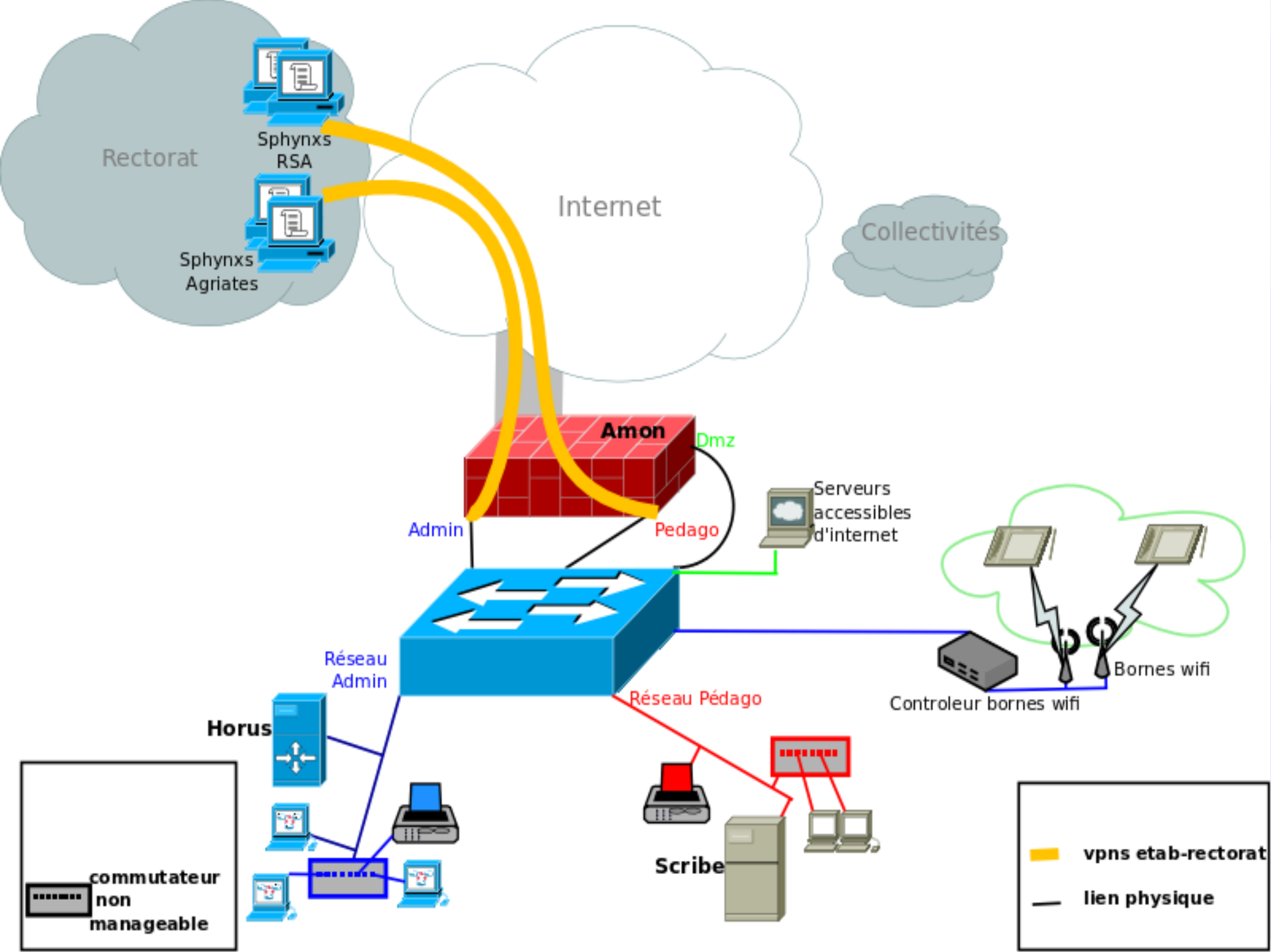
- Pas plus de 4 zones physiques (externe, administration, pédagogique, dmz)



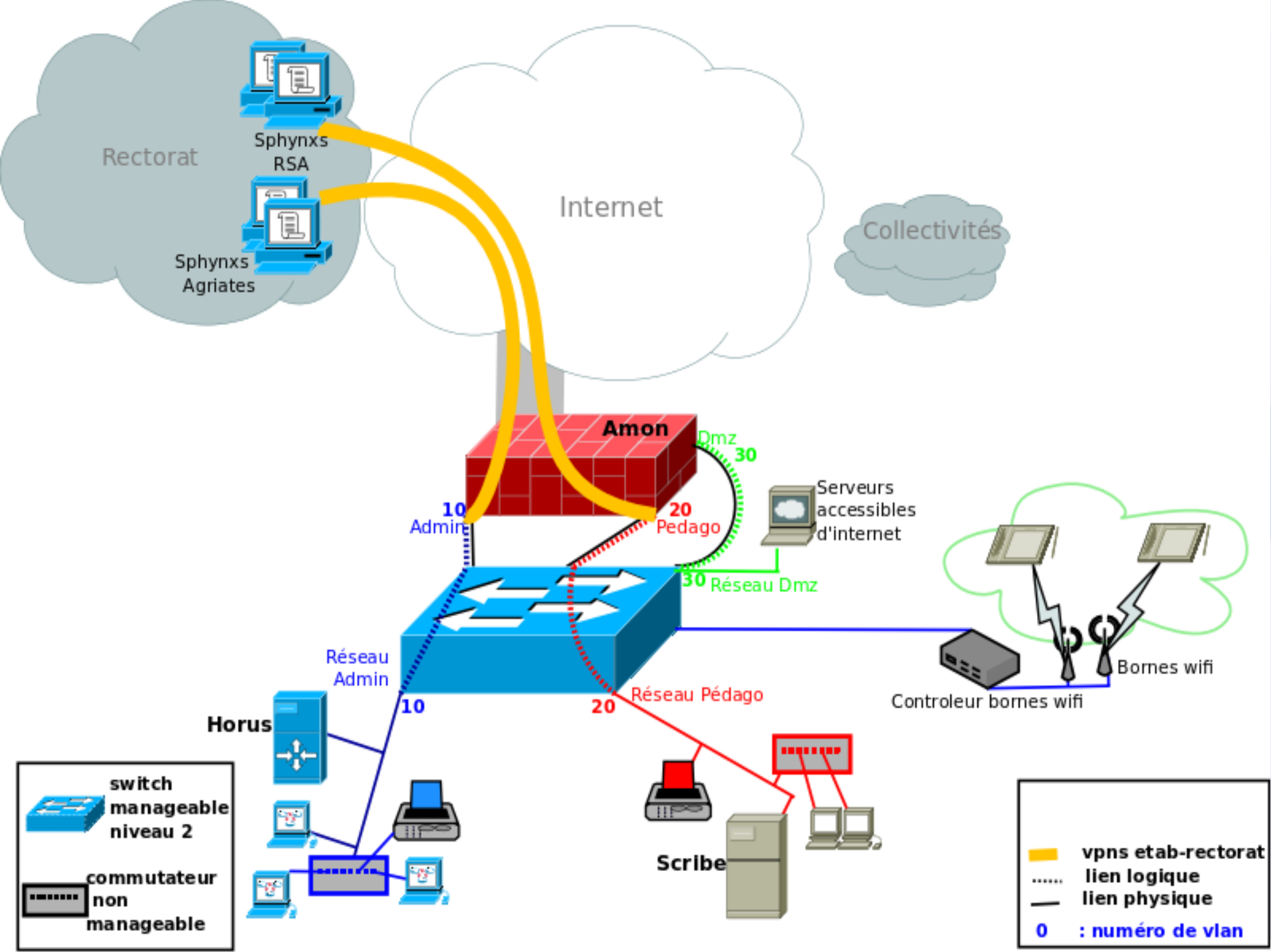
Utilisation de vlans de niveau 1 (par port)



Ajout d'un switch de niveau 2 entre l'Amon et les sous-réseaux

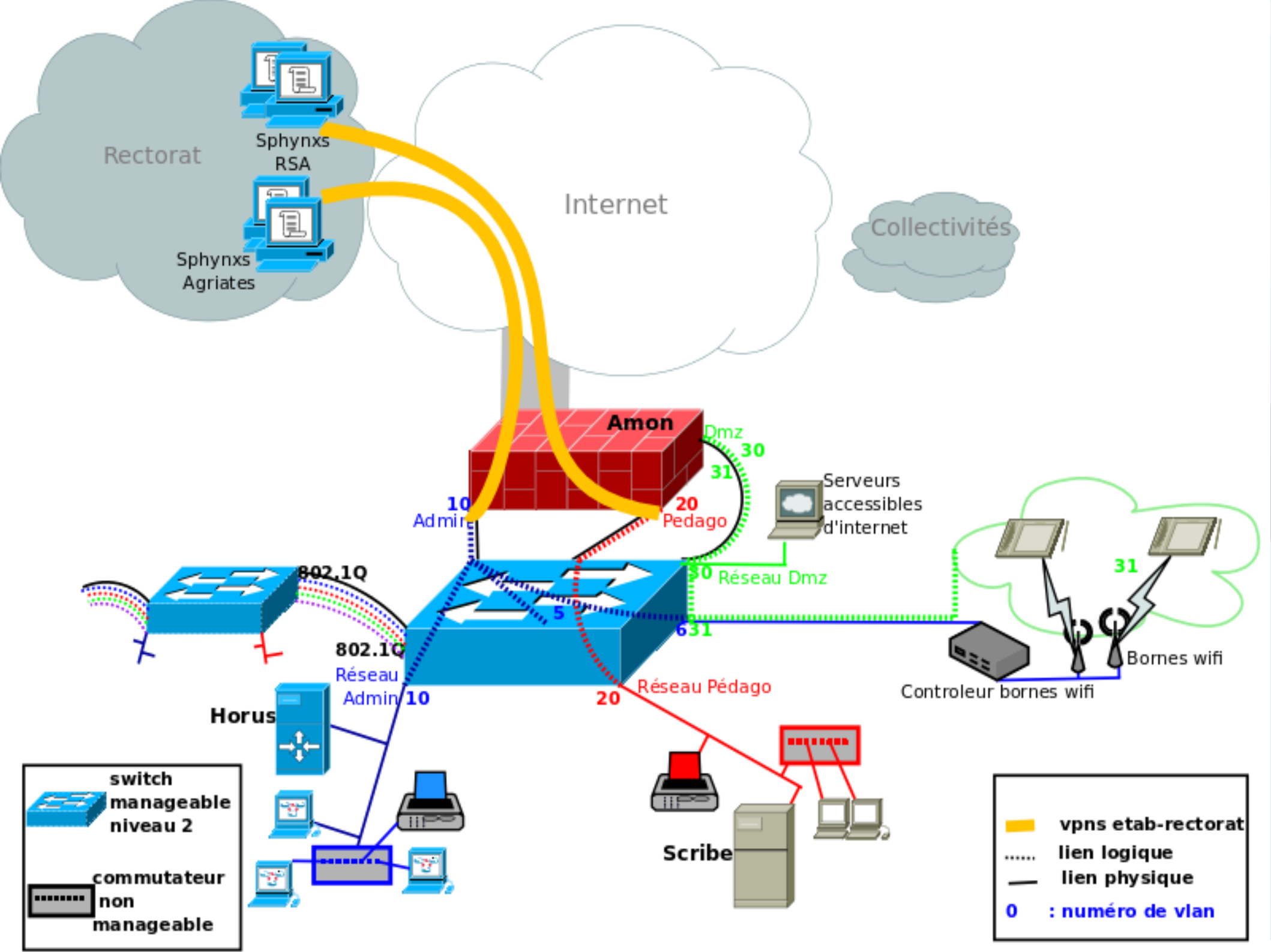

Rectorat
Sphynxs
RSA
Sphynxs
Agriates
Internet
Collectivités
Amon
Dmz
Admin
Pedago
Serveurs
accessibles
d'internet
Réseau
Admin
Réseau Pédago
Horus
Scribe
Controleur bornes wifi
Bornes wifi
commutateur
non
manageable
vpns etab-rectorat
lien physique

- Généralisation des vlans à tous les sous-réseaux et aux interfaces de l'Amon : définition d'un nouveau modèle académique « full_vlans.xml »


Rectorat
Sphynxs
RSA
Sphynxs
Agriates
Internet
Collectivités
Amon
Dmz
30
10
Admin
20
Pedago
Serveurs
accessibles
d'internet
30
Réseau Dmz
Réseau
Admin
10
20
Réseau Pédago
Horus
Scribe
Bornes wifi
Controleur bornes wifi
switch
manageable
niveau 2
commutateur
non
manageable
vpns etab-rectorat
lien logique
lien physique
0 : numéro de vlan

Intérêts de cette structure

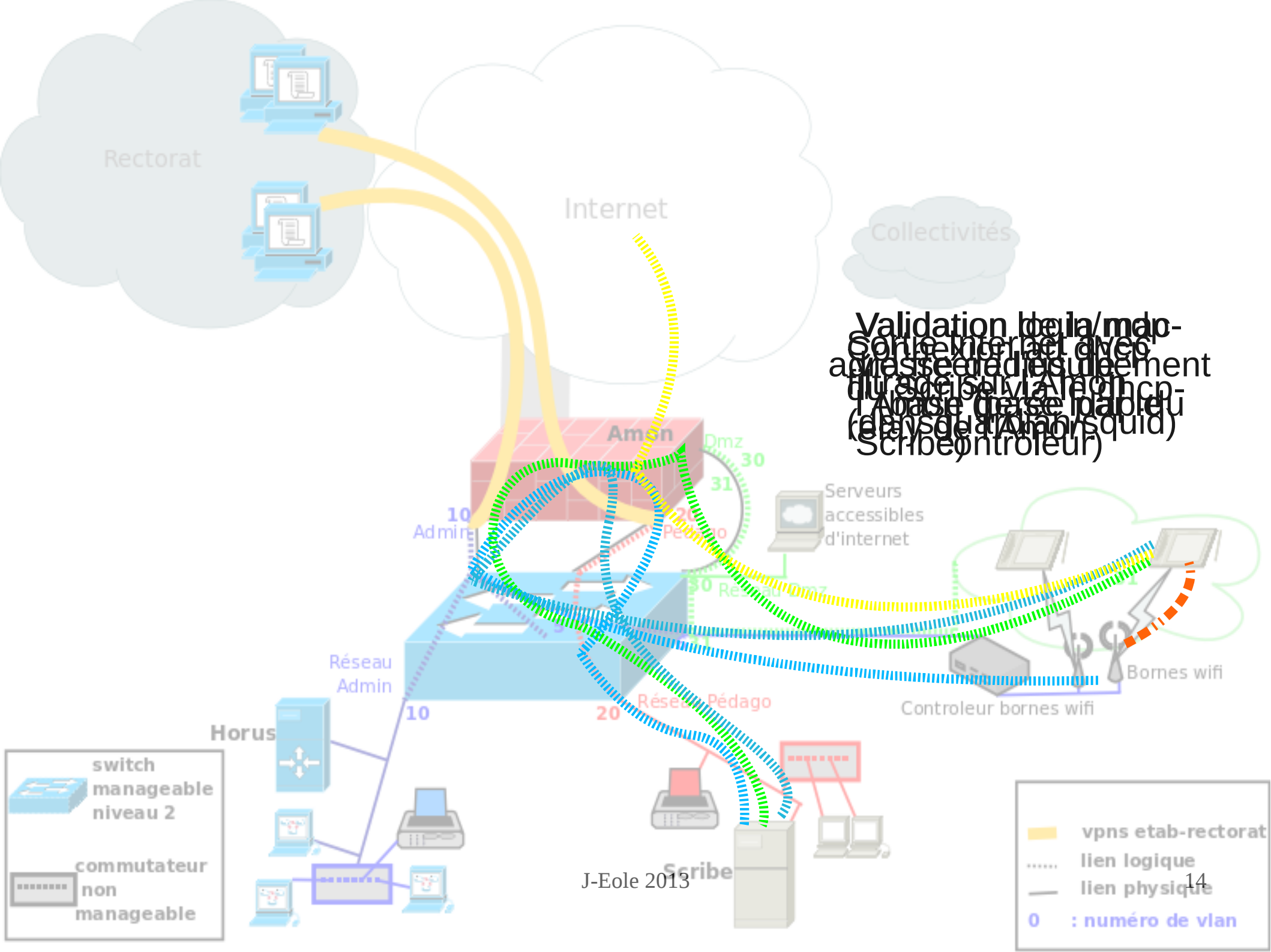
- Étanchéité des flux
- Extensibilité sans limites
- Utilisation du dhcp relay pour les équipements wifi (bornes, tablettes) : patchs sur dcp-relay de l'Amon et dhcpd.conf du scribe
- Supervision des infrastructures (réseaux, wifi) depuis une zone adriatic (outil IMC d'HP)
-


Rectorat
Sphynxs
RSA
Sphynxs
Agriates
Internet
Collectivités
Amon
Dmz
30
31
10
Admin
20
Pedago
Serveurs
accessibles
d'internet
802.1Q
30
Réseau Dmz
5
31
802.1Q
Réseau
Admin 10
20
Réseau Pédago
Horus
Scribe
Controleur bornes wifi
Bornes wifi
31
switch
manageable
niveau 2
commutateur
non
manageable
vpns etab-rectorat
lien logique
lien physique
0 : numéro de vlan

- Utilisation de Freeradius pour valider dans la base ldap du Scribe le login/mdp :
  - Patchs nombreux en 2.2
    - freerad-users, freerad-clients, freerad-default, freerad-ldap, radiusd
  - Intégré en 2.3 si on passe l'onglet freeradius en mode « accounting »

Attention : obligation de saisir le .reader du Scribe en dur dans la conf (problème potentiel en cas de changement de Scribe)

- Si l'infrastructure réseau locale le permet, on peut propager le 802.1Q sur tout l'établissement :
  - Connexion d'un poste à un sous-réseau indépendamment de sa position géographique
  - Placement optimale des bornes wifi POE pour une couverture globale
  - GTC facilitée


Rectorat
Internet
Collectivités
Validation de la mac-
adresse directement
(dans l'Annuaire)
Amon
Dmz
30
31
10
Admin
20
Pédago
Serveurs
accessibles
d'internet
Réseau
Admin
10
Réseau Pédago
20
Horus
Bornes wifi
Controleur bornes wifi
Scribe
switch
manageable
niveau 2
commutateur
non
manageable
vpns etab-rectorat
lien logique
lien physique
0 : numéro de vlan

- Mise en place de l'accounting sur Freeradius pour les connexions wifi (couple login – horaire de connexion) en mode sql pour n'avoir qu'un fichier :

  /var/log/freeradius/radacct/sql-relay

- Rotation hebdomadaire de ce fichier avec historique sur un an :
  - modification de /etc/logrotate.d/freeradius

- En cas de requête judiciaire sur un accès Internet depuis l'établissement :
  - Si l'adresse ip source incriminée (dans l'access.log du squid) appartient au réseau « wifi » (qui n'est pas authentifié),
  - on peut retrouver le login de la personne connectée avec cette ip et à l'heure dite dans le sql-relay de freeradius

Extraits de logs Wifi

Fichier sql-relay :

(SessionId,UserName,NASIPAddress,FramedIPAddress,AcctStartTime,AcctStopTime,Duration)

('***-061','prenom.nom', '10.90.119.148','172.20.0.66','2013-09-30 09:06:43','0', '0', '')

('***-061','prenom.nom','10.90.119.148','172.20.0.66','0','2013-09-30 09:55:19','2916','')

Access .log du squid :

Sep 30 09:50:31 pf-amon squid[3962]: 1380527731.855 41 172.20.0.66 TCP_MISS/200 332 GET http://gsp1.apple.com/pep/gcc - DIRECT/193.51.224.48 text/html

Wifi : conditions

	Environnements	
	Mono-Utilisateurs	Multi-Utilisateurs
Type de terminal	Tablettes, Phablettes, Smartphone	Notebook, Netbook, Tablettes
Systèmes d'exploitation	Android, iOS	Microsoft Windows
Authentification NTLM	Non géré en natif	Compatibilité avec les versions Professionnelles uniquement
Wi-Fi sur réseau ADMIN	Usage INTERDIT	Usage INTERDIT
Wi-Fi sur réseau PEDAGO	Non fonctionnel (cf. non prise en charge native de la couche NTLM)	Toléré à titre exceptionnel (cf. « Mise en œuvre d'un réseau Wi-Fi connecté au réseau Pédagogique »)
Wi-Fi sur réseau dédié	Usage recommandé	Usage recommandé

Conclusion

- Utilisation actuellement maîtrisée du wifi dans des établissement scolaires :
  - OS multi-utilisateurs ou matériel personnel

    ET
  - Matériel validé et connu (bridage mac-adresses)
- Perspectives :
  - BYOD (portail captif?)

Merci de votre attention

Des questions ?

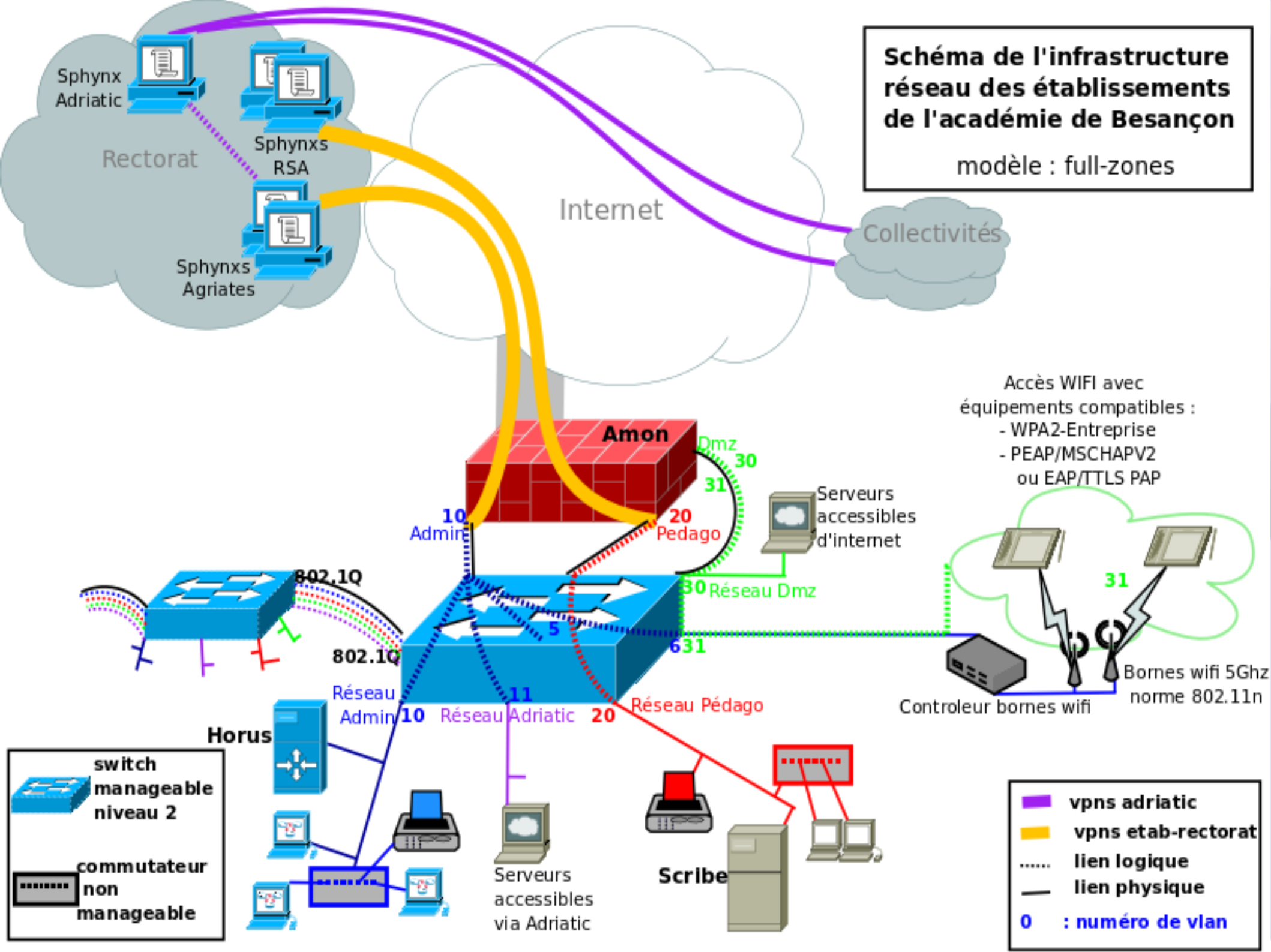


Schéma de l'infrastructure réseau des établissements de l'académie de Besançon
modèle : full-zones
Sphynx Adriatic
Rectorat
Sphynxs RSA
Sphynxs Agriates
Internet
Collectivités
Amon
Dmz
30
31
10
Admin
20
Pedago
Serveurs accessibles d'internet
Accès WIFI avec équipements compatibles :
- WPA2-Entreprise
- PEAP/MSCHAPV2
ou EAP/TTLS PAP
802.1Q
802.1Q
30
Réseau Dmz
5
631
31
Bornes wifi 5Ghz norme 802.11n
Controleur bornes wifi
Réseau Admin
10
11
Réseau Adriatic
20
Réseau Pédago
Horus
Serveurs accessibles via Adriatic
Scribe
switch manageable niveau 2
commutateur non manageable
vpns adriatic
vpns etab-rectorat
lien logique
lien physique
0 : numéro de vlan