


DATA TEMPLAR

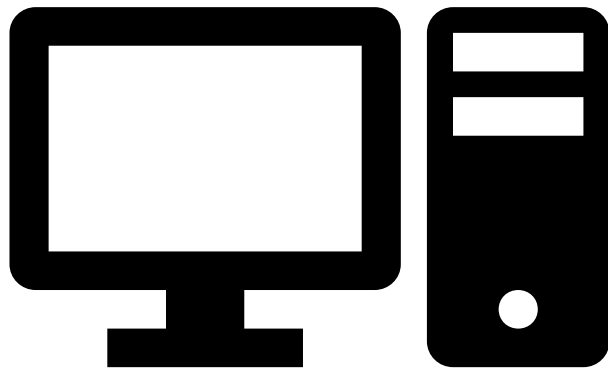
Mission SI : Le système d'information
et ses composants de sécurité

PRÉSENTÉ PAR QUENTIN BÉDÉNEAU ET FLORIAN STOSSE



Le système d'information

Un ordinateur



Applications



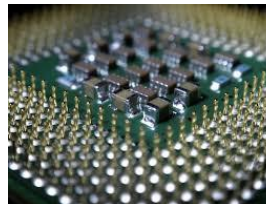
OS



Firmware



Couche physique



Plus d'informations:
<http://www.comptons.com/fr>
Images: stockphoto.com

Terminaux

Postes clients

IoT

Alarmes / vidéo-surveillance

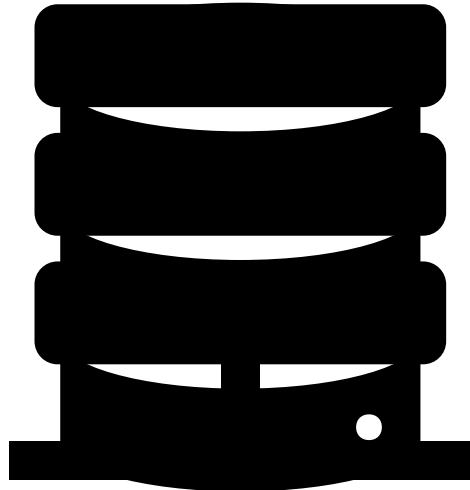
Imprimantes

Ordiphones

Postes nomades

Machines à café (hé oui !)

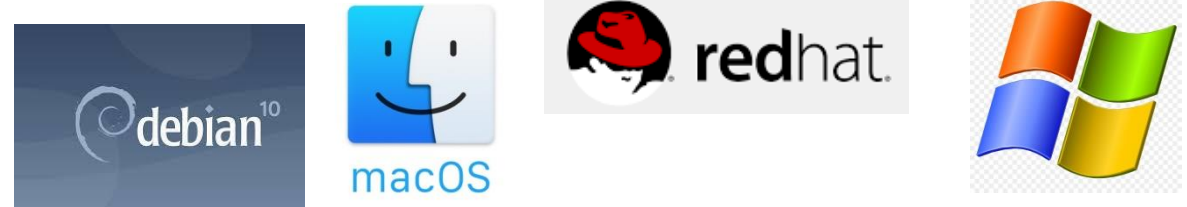
Le serveur



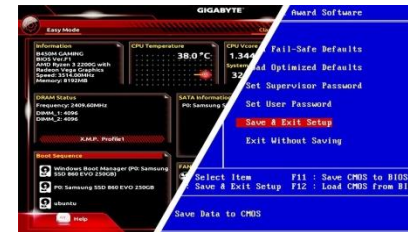
Applications



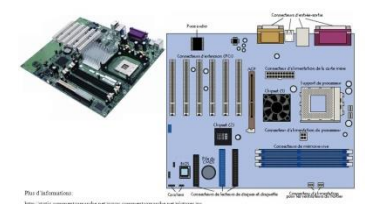
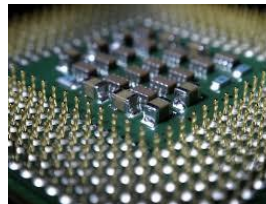
OS



Firmware



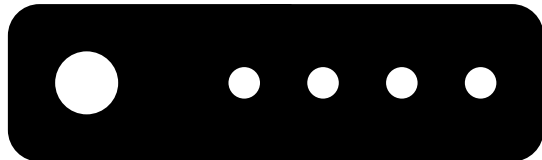
Couche physique



Le réseau

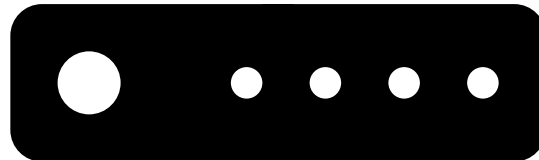
Le switch

Crée un réseau entre ordinateurs



Le routeur

Crée un réseau entre réseaux



Le routeur Wifi

Crée un réseau sans fil. Fait office de switch et de routeur



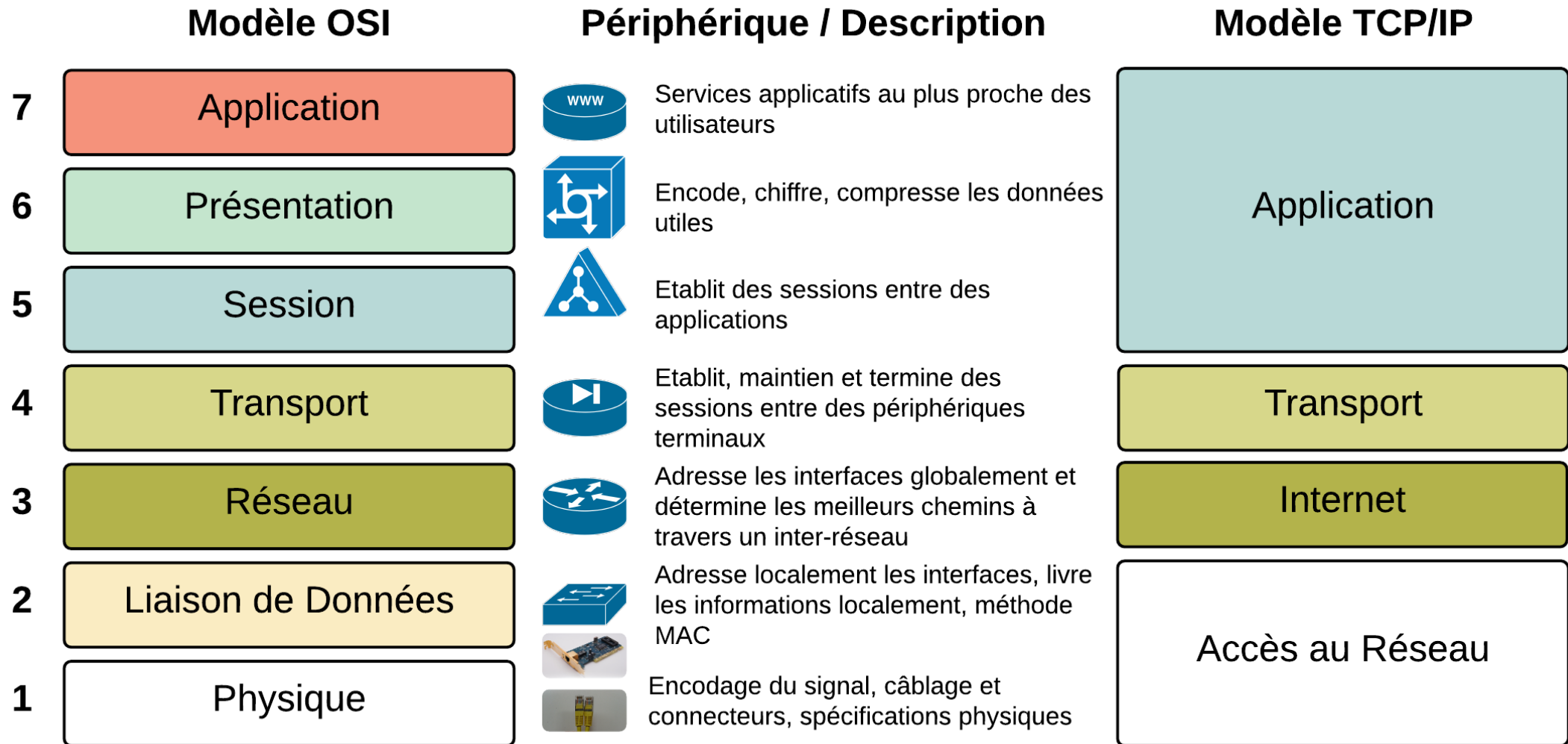


IT is *like onions*

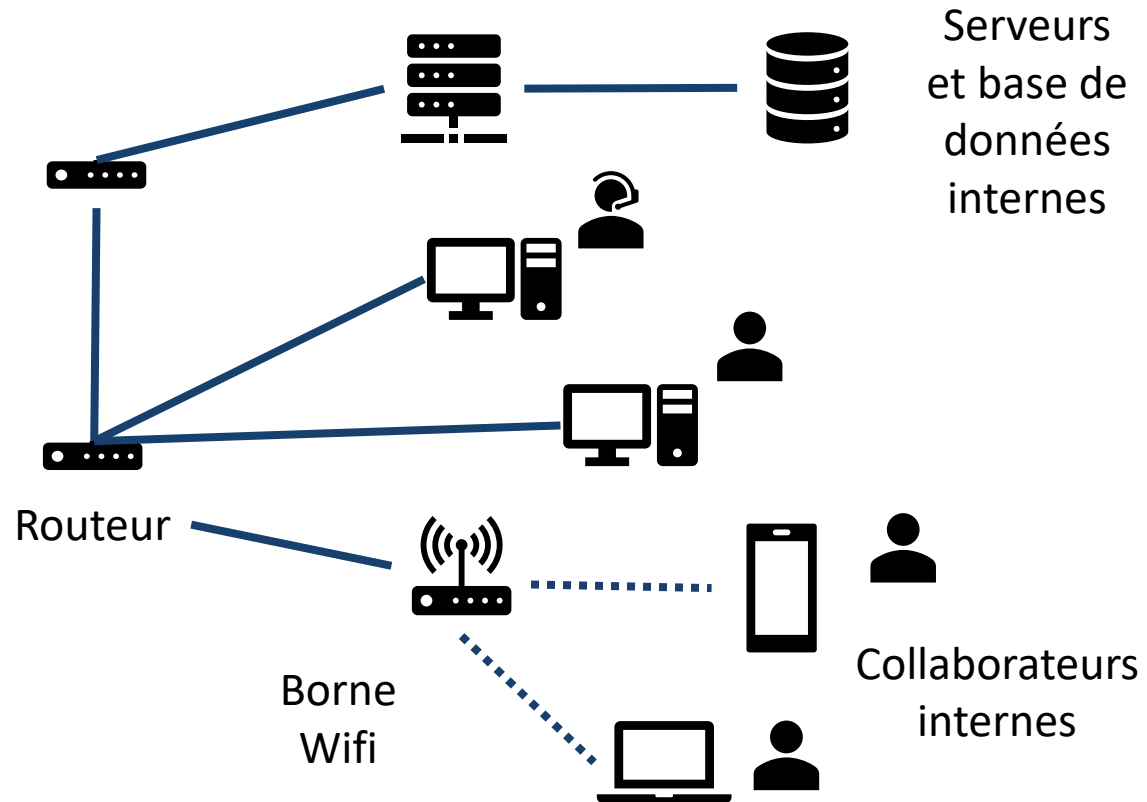


NO. Layers. Onions have layers.

Le modèle OSI



Modélisation d'un SI

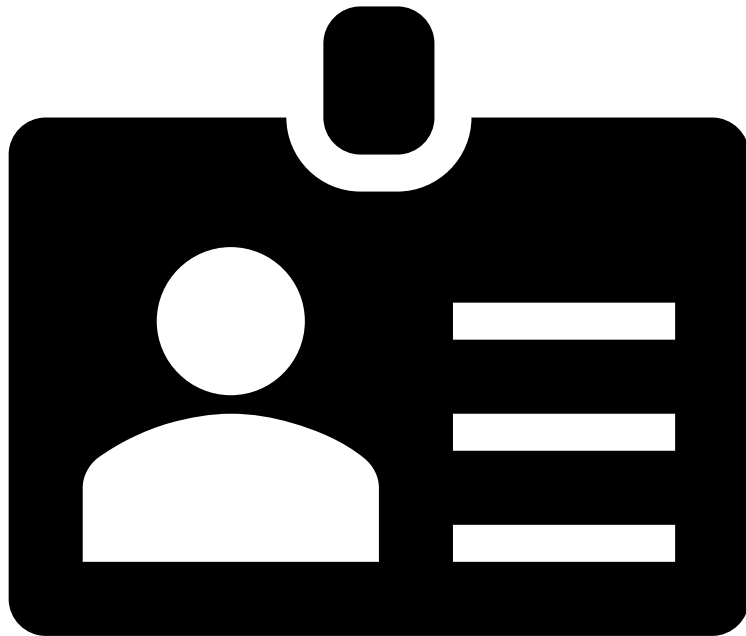




Les composants de sécurité

Pour le réseau interne

Annuaire d'entreprise (LDAP ou Active Directory)

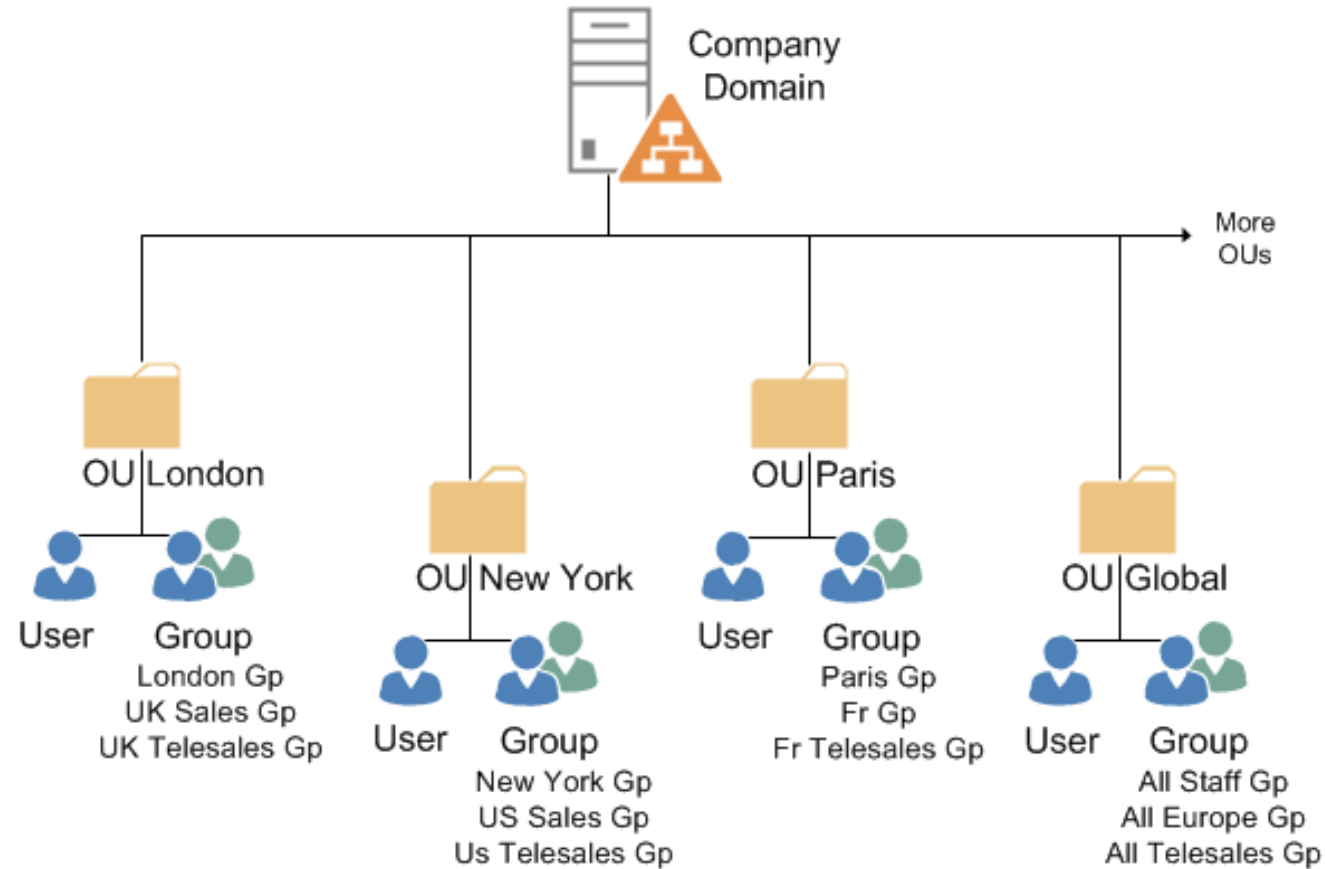


LDAP est un protocole, par abus de langage, on le considère comme une application d'annuaire.

Active Directory est une implémentation de Microsoft.

Gère l'identité des utilisateurs ainsi que leurs droits.

Annuaire d'entreprise (LDAP ou Active Directory)



Malware protection

Protège contre les logiciels malveillants

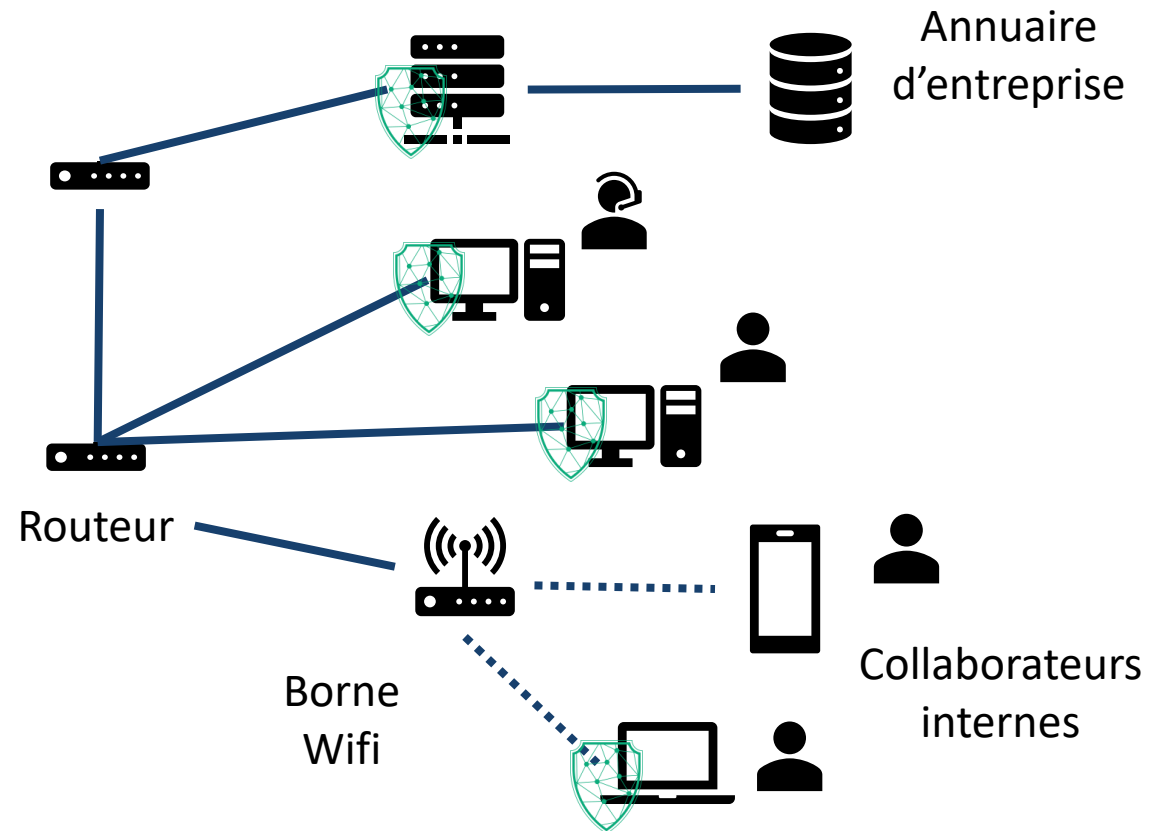
Virus = malware = adware...

Cherche dans les fichiers des éléments connus (Signatures ou Indicateurs de compromission IOC)

« Analyse comportementale » pour les plus puissant



Où mettre l'antivirus?



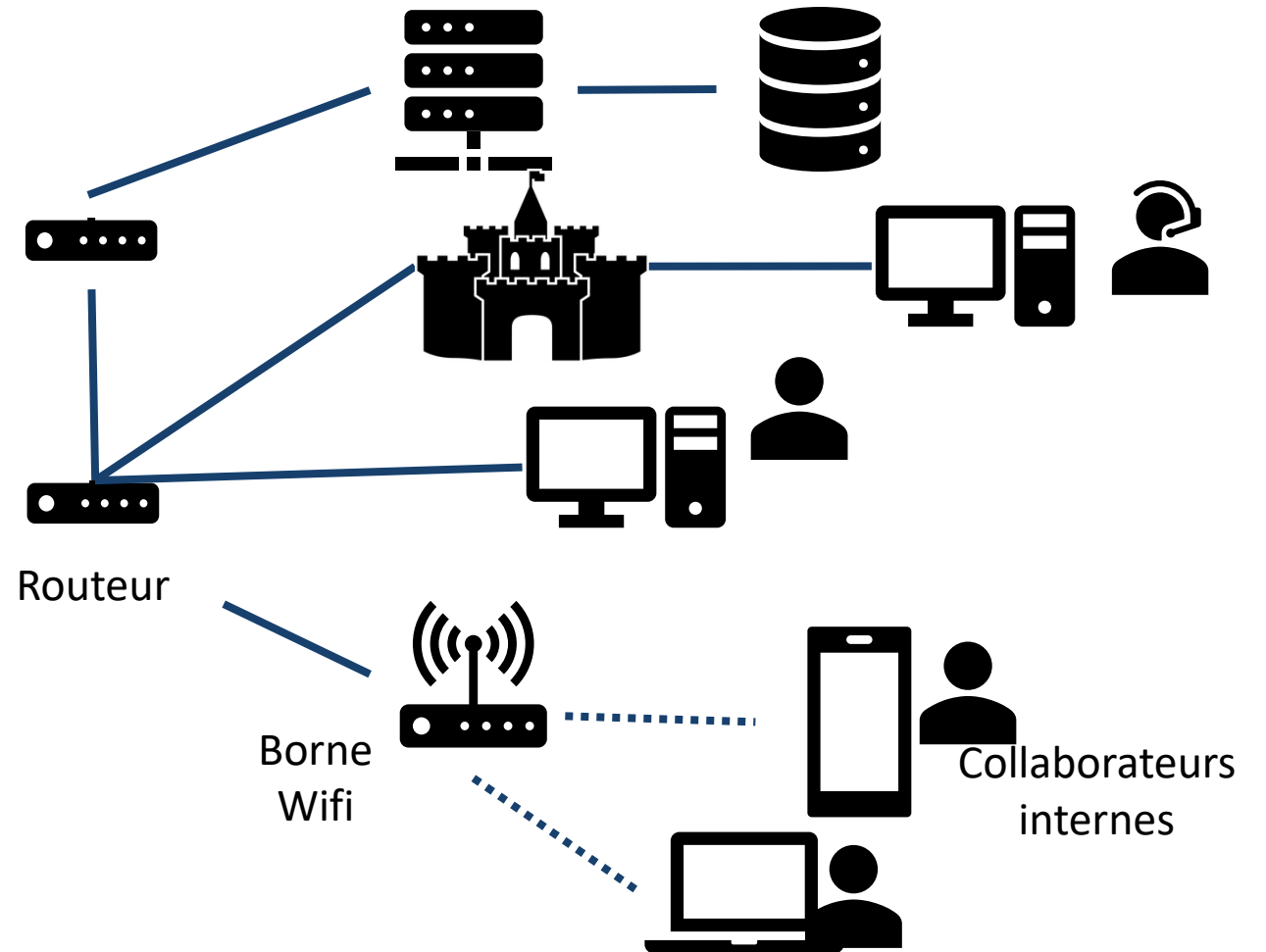
SIEM



Bastion

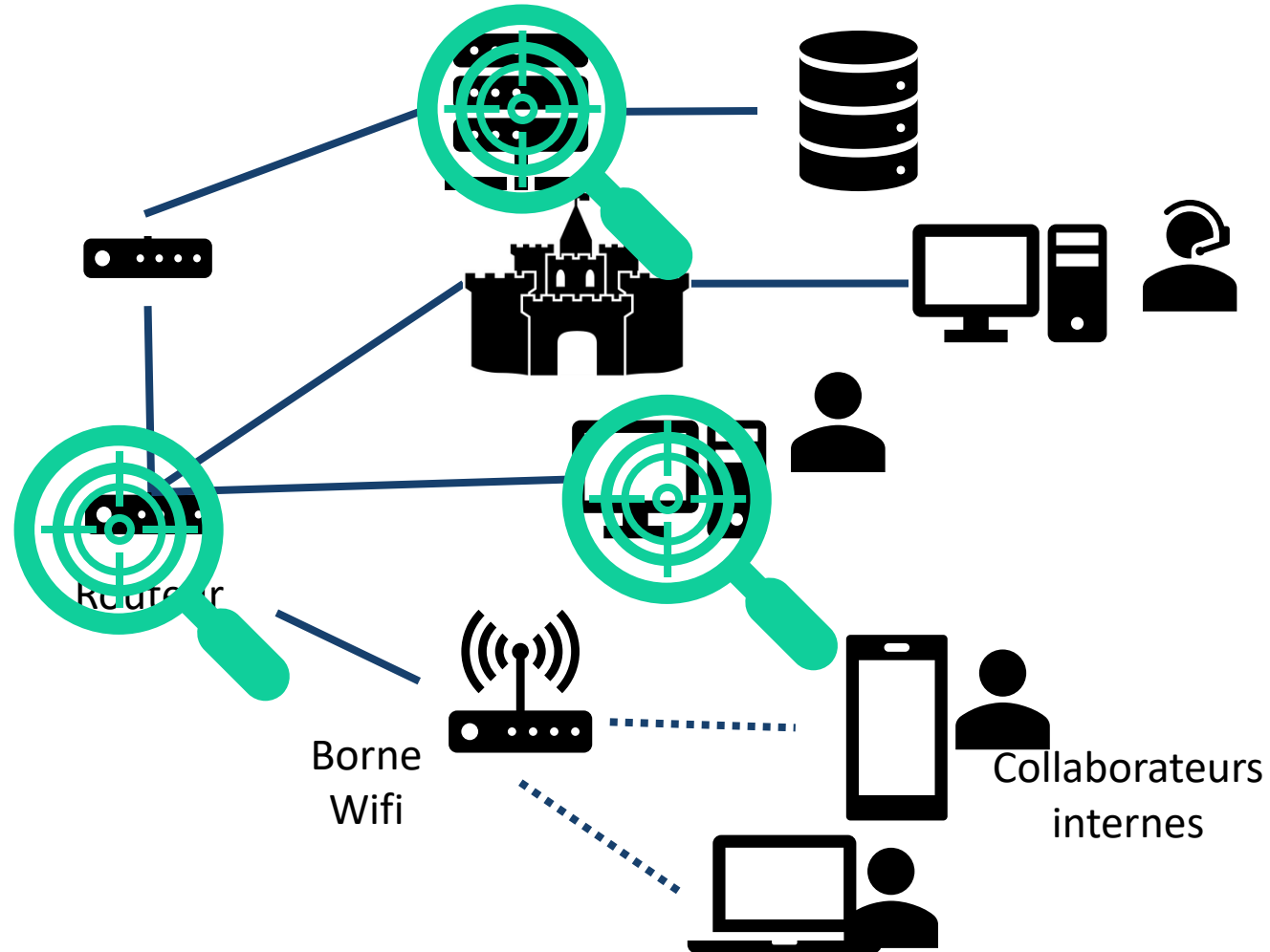
Le bastion permet de superviser et contrôler les administrateurs

Il va être l'unique moyen d'authentification autorisé et enregistrera toutes les activités réalisées



Scanner de vulnérabilités

Fonctionne via
des scripts pour
trouver des
vulnérabilités
connues



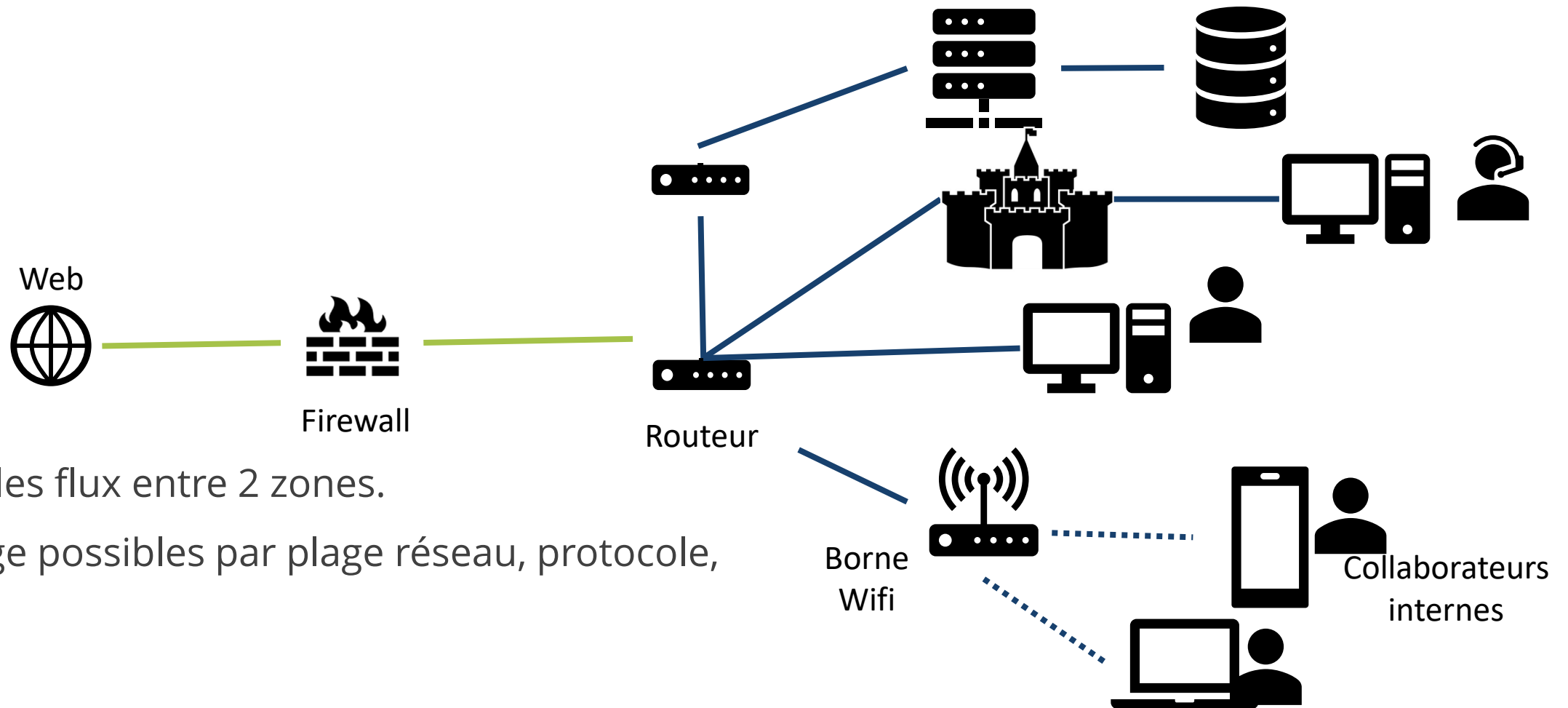


Les composants de sécurité

Pour le réseau externe.

Connexion à l'Internet en
cours...

Firewall



Filtre les flux entre 2 zones.

Filtrage possibles par plage réseau, protocole, port

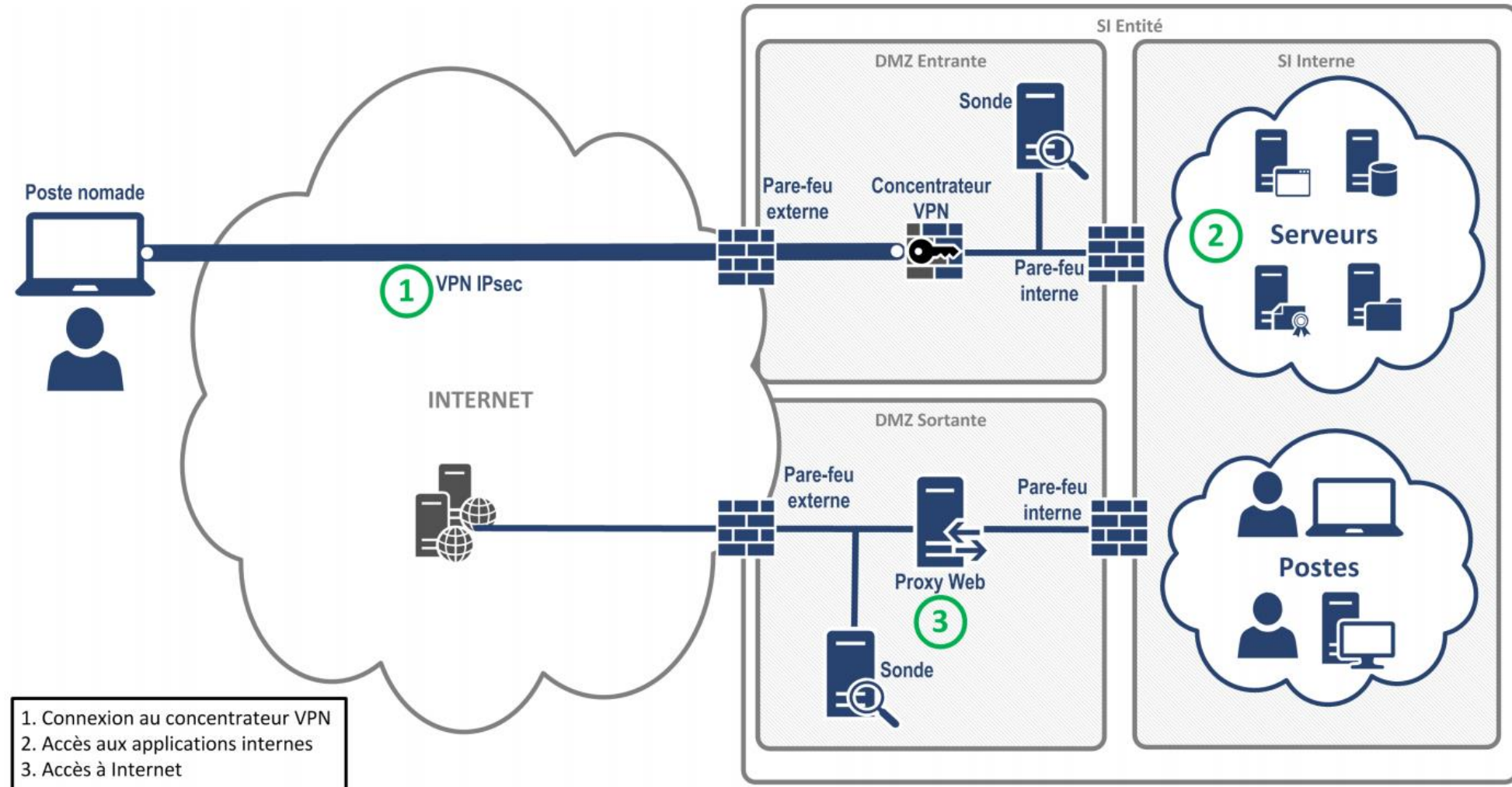
Firewall



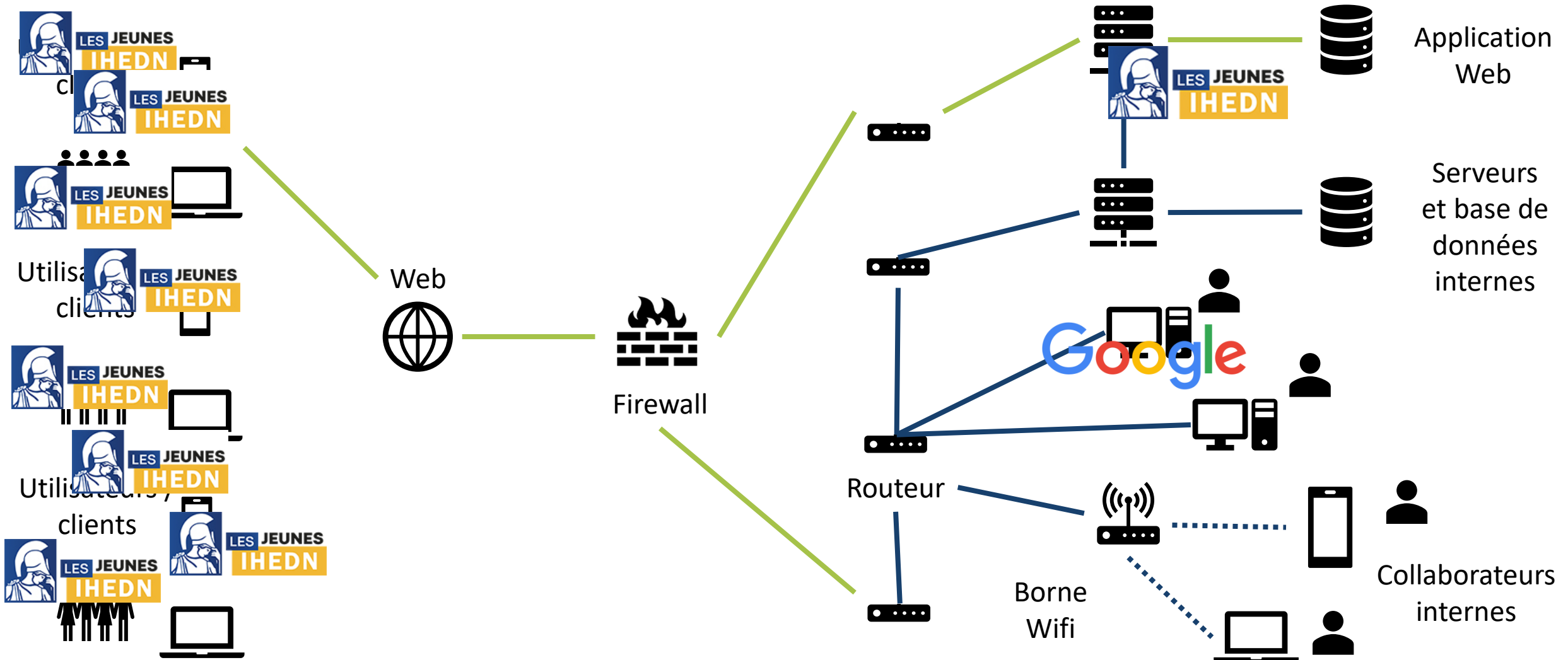
USG9520



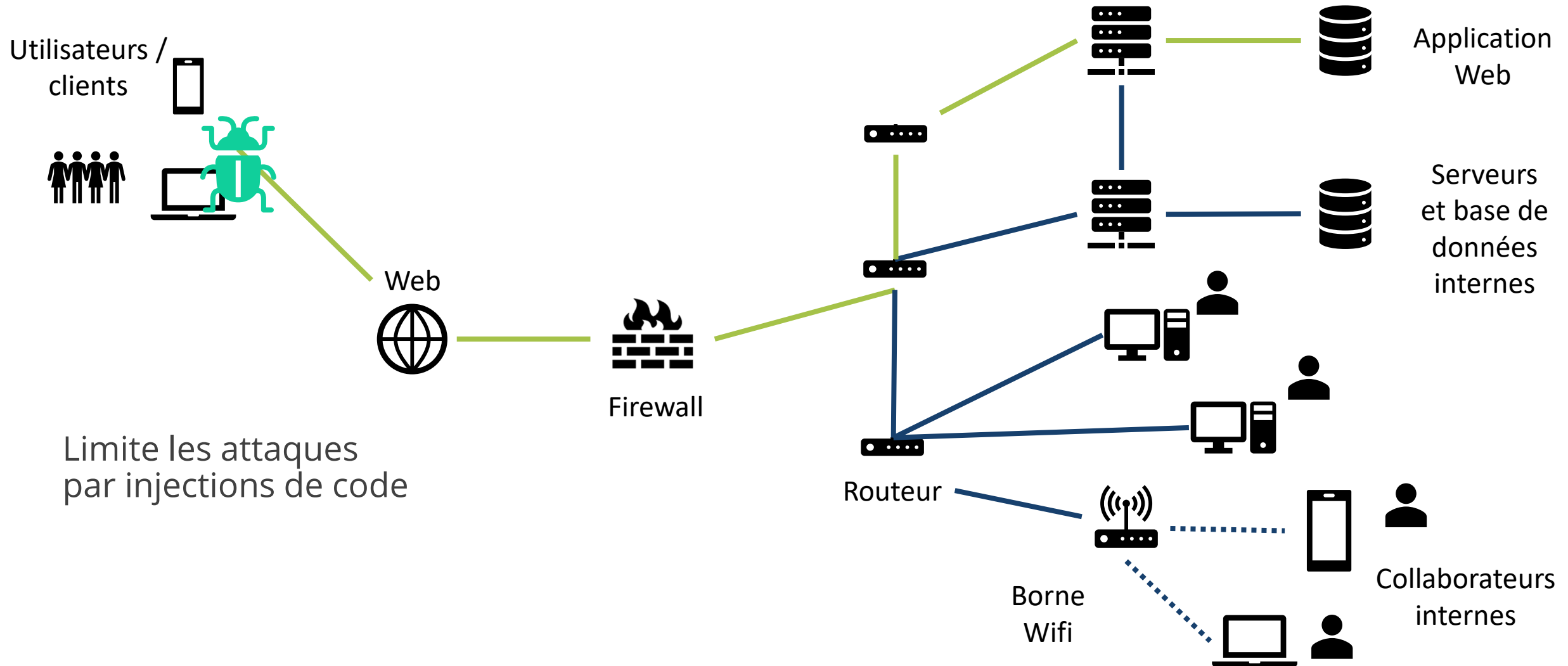
VPN



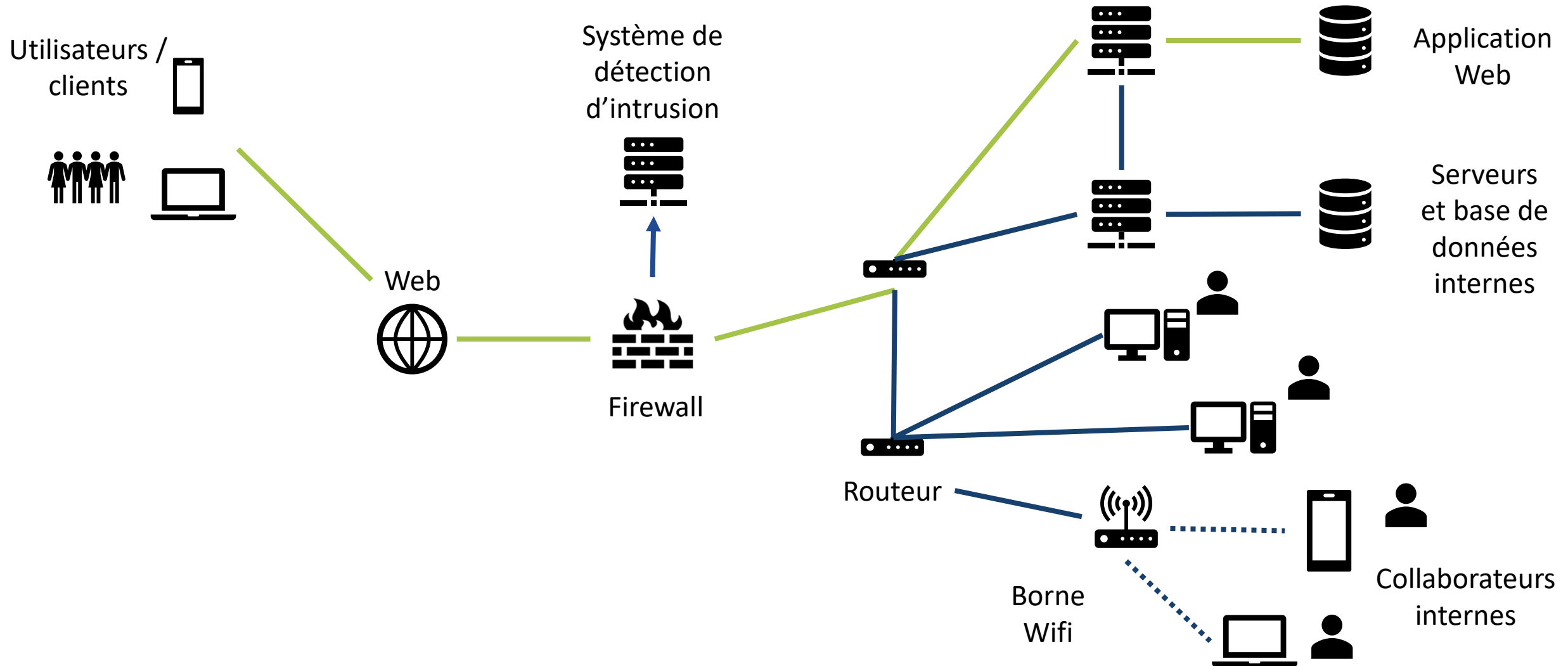
Proxy/Reverse proxy



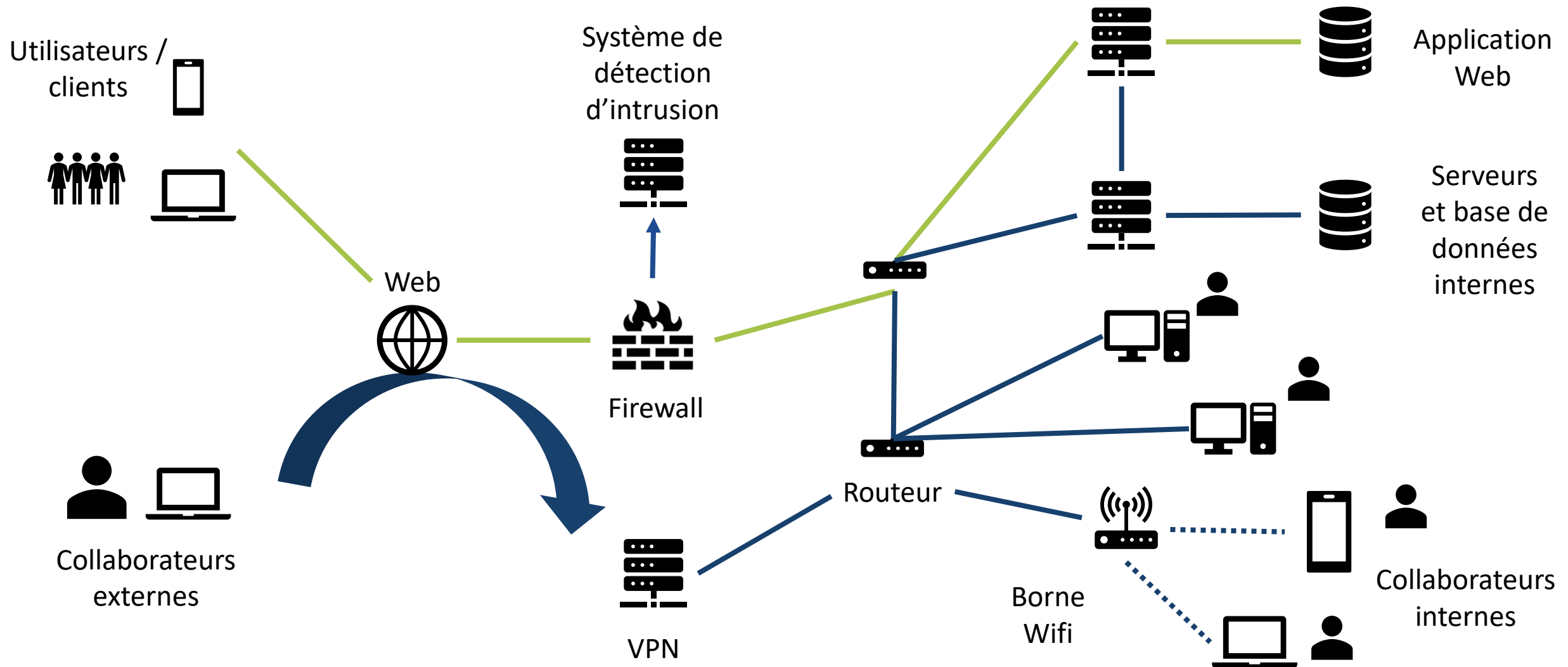
Web Application Firewall (WAF)



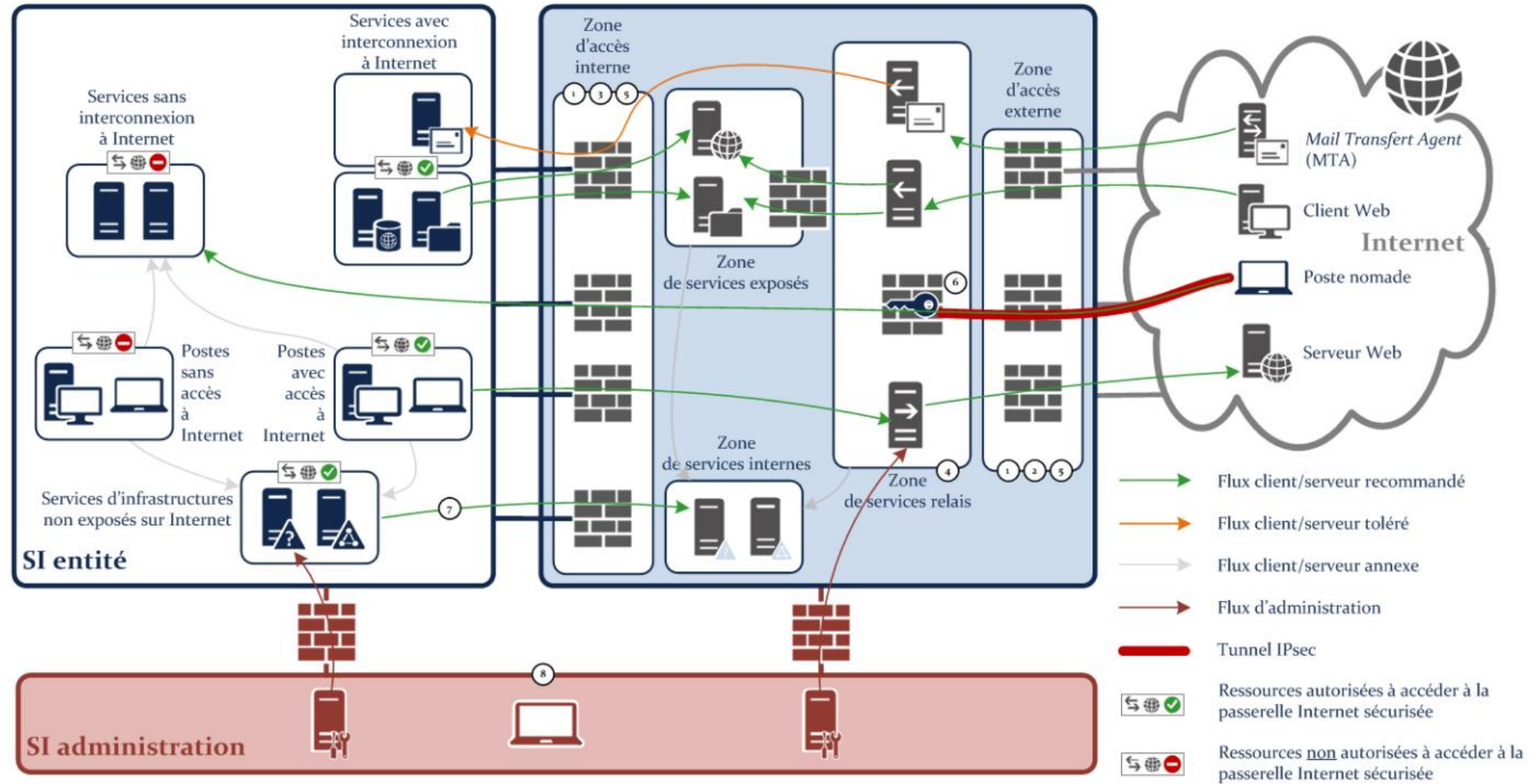
IDS/IPS



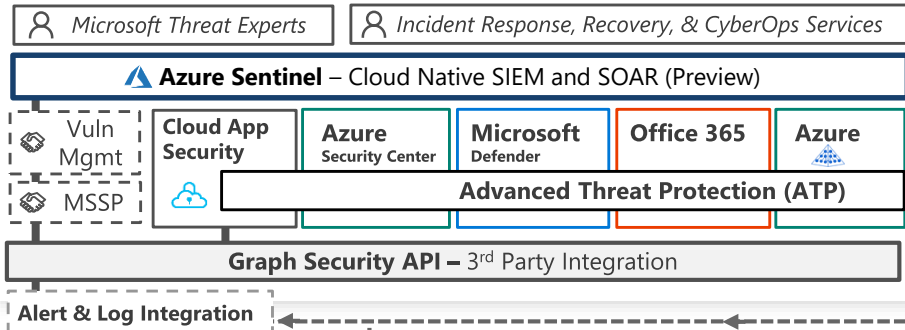
Modélisation d'un SI



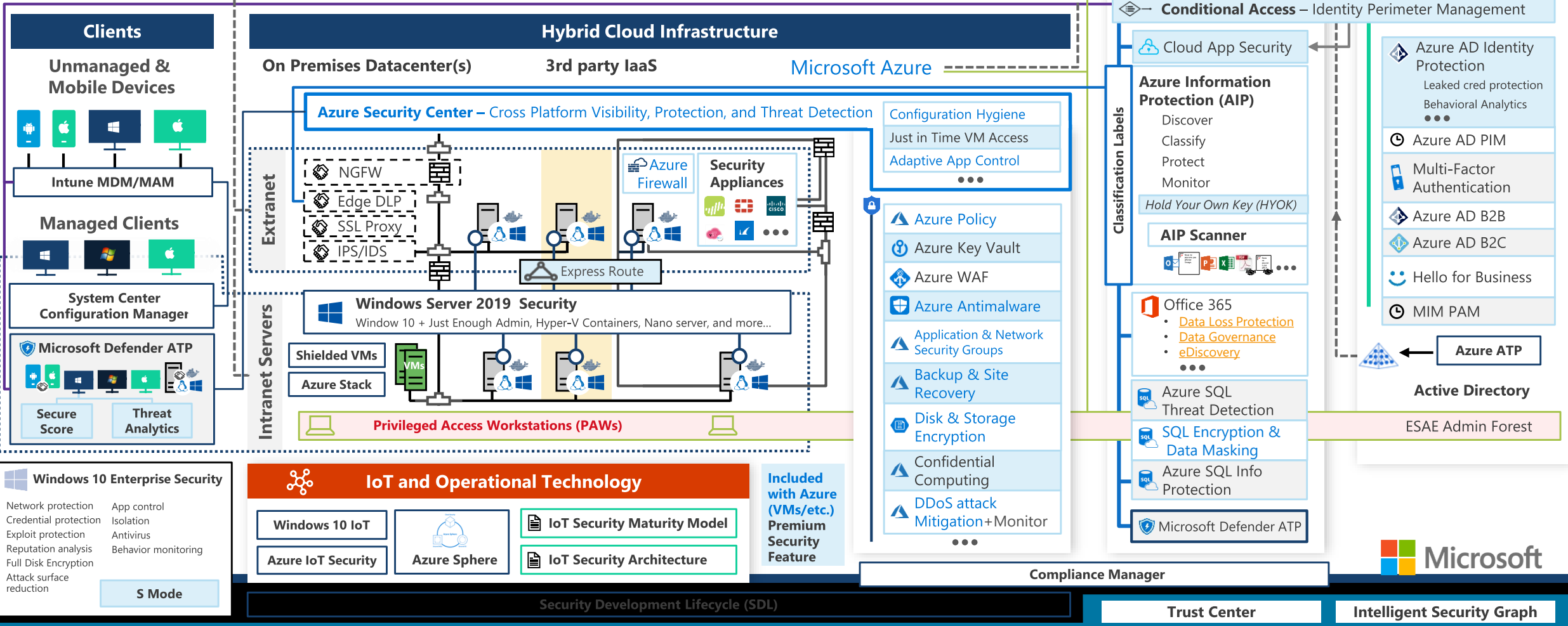
Architecture de référence (ANSSI)



Security Operations Center (SOC)



Architecture Cloud de référence (Microsoft Azure)



Contacts



LES JEUNES
IHEDN
L'association

Comité Cyber:

- Mail : cyber@anaj-ihedn.org

Quentin Bédéneau

- Twitter : @data_qyou
- Mail : quentin@datatemplar.fr

Florian Stosse

- Twitter : @Harvesterify
- Mail : florian.stosse@gmail.com

Sources

<https://www.commentcamarche.net/>

<https://cisco.goffinet.org/ccna/fondamentaux/modeles-tcp-ip-osi/>

<https://openclassrooms.com/fr/>

<https://www.wikipedia.org/>

Architecture de référence ANSSI :

<https://www.ssi.gouv.fr/entreprise/guide/definition-dune-architecture-de-passerelle-dinterconnexion-securisee/>

VPN :

<https://www.ssi.gouv.fr/entreprise/guide/recommandations-sur-le-nomadisme-numerique/>

Microsoft Cybersecurity Reference Architecture :

<https://gallery.technet.microsoft.com/Cybersecurity-Reference-883fb54c>