RÉPUBLIQUE TUNISIENNE
MESRS
Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

مركز الحساب الخوارزمي
Centre de Calcul El-Khawarizmi
إدارة الإستغلال و الخدمات

مركز الحساب الخوارزمي
Centre de Calcul El-Khawarizmi

Le CCK de 1976 à 2022

Depuis 1976, au service de l'enseignement supérieur et la recherche scientifique

Depuis 1997 fournisseur des service internet pour le secteur du l'ESRS

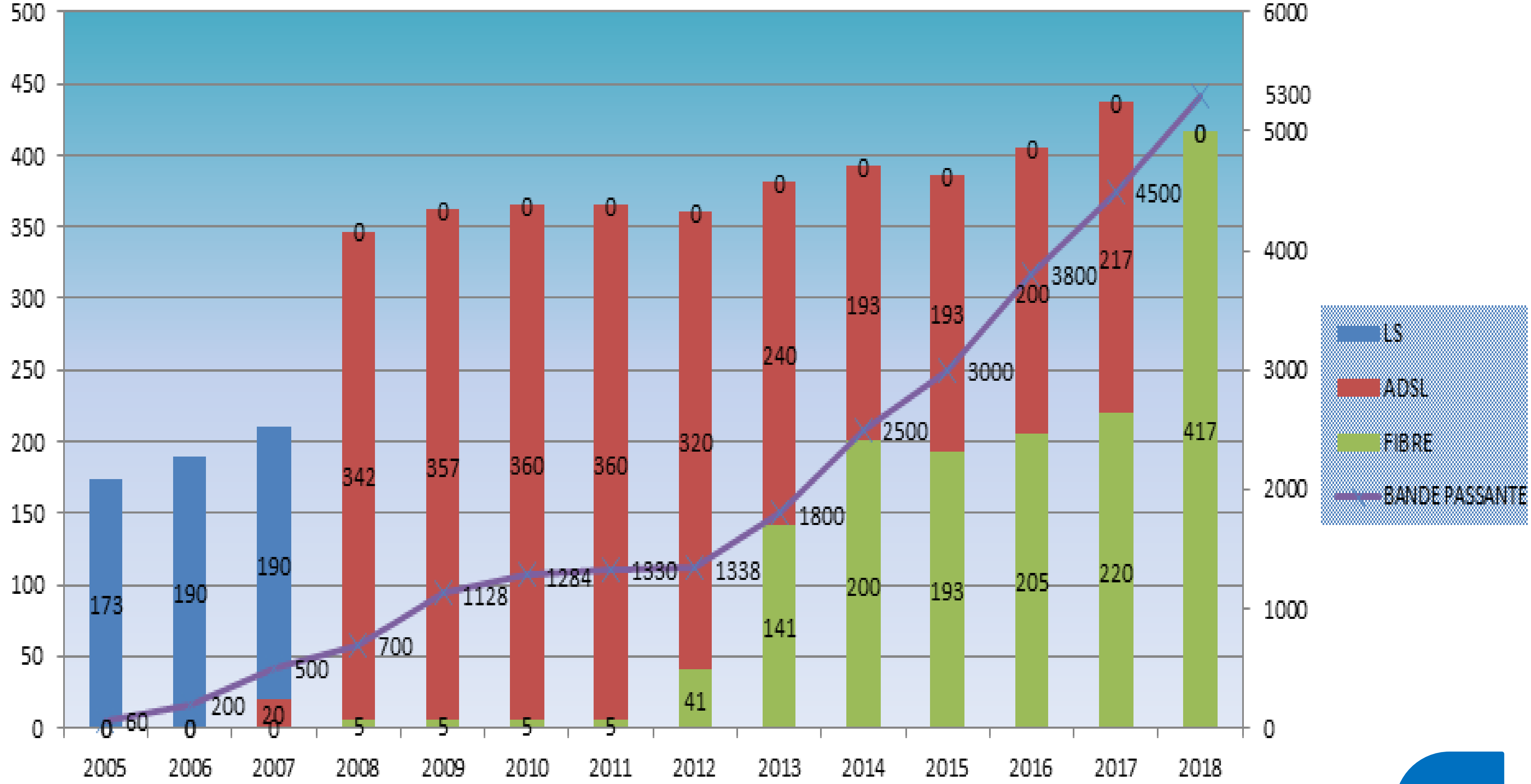
LE CCK

- Créé en 1976
- Depuis 1997 - FSI : le Fournisseur de Services Internet Pour le secteur de l'ESRS
- Direction Générale au MESRS
- Local principal au Campus universitaire de la manouba depuis 2004
- Local secondaire au Campus universitaire du manar
- Ressources humaines : 55 membres = 08 ingénieurs + 12 techniciens + 10 administrateurs + 25 autres

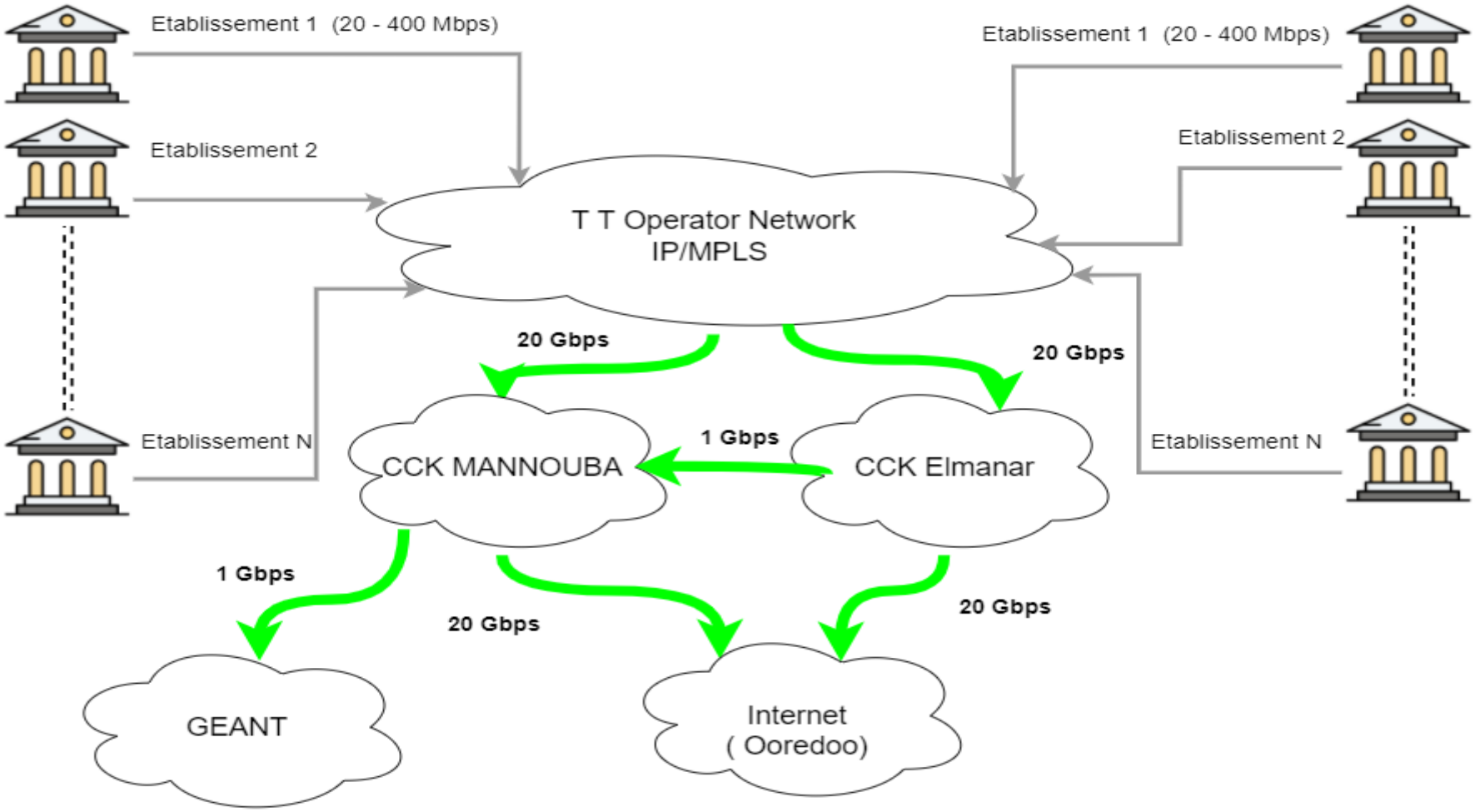
MISSION DEPUIS 2005

- Décret no. 2005-50 du 10 Janvier 2005.
  - Le CCK a pour mission d'organiser, de promouvoir, d'assurer et d'encourager l'utilisation des technologies numériques dans le milieu universitaire et scientifique en général.
  - Il est chargé aussi de la recherche dans ce domaine en vue d'améliorer l'utilisation de la technologie informationnelle numérique dans le milieu universitaire ainsi qu'au profit des enseignants et des étudiants.

Network infrastructure and bandwidth 2005 - 2018

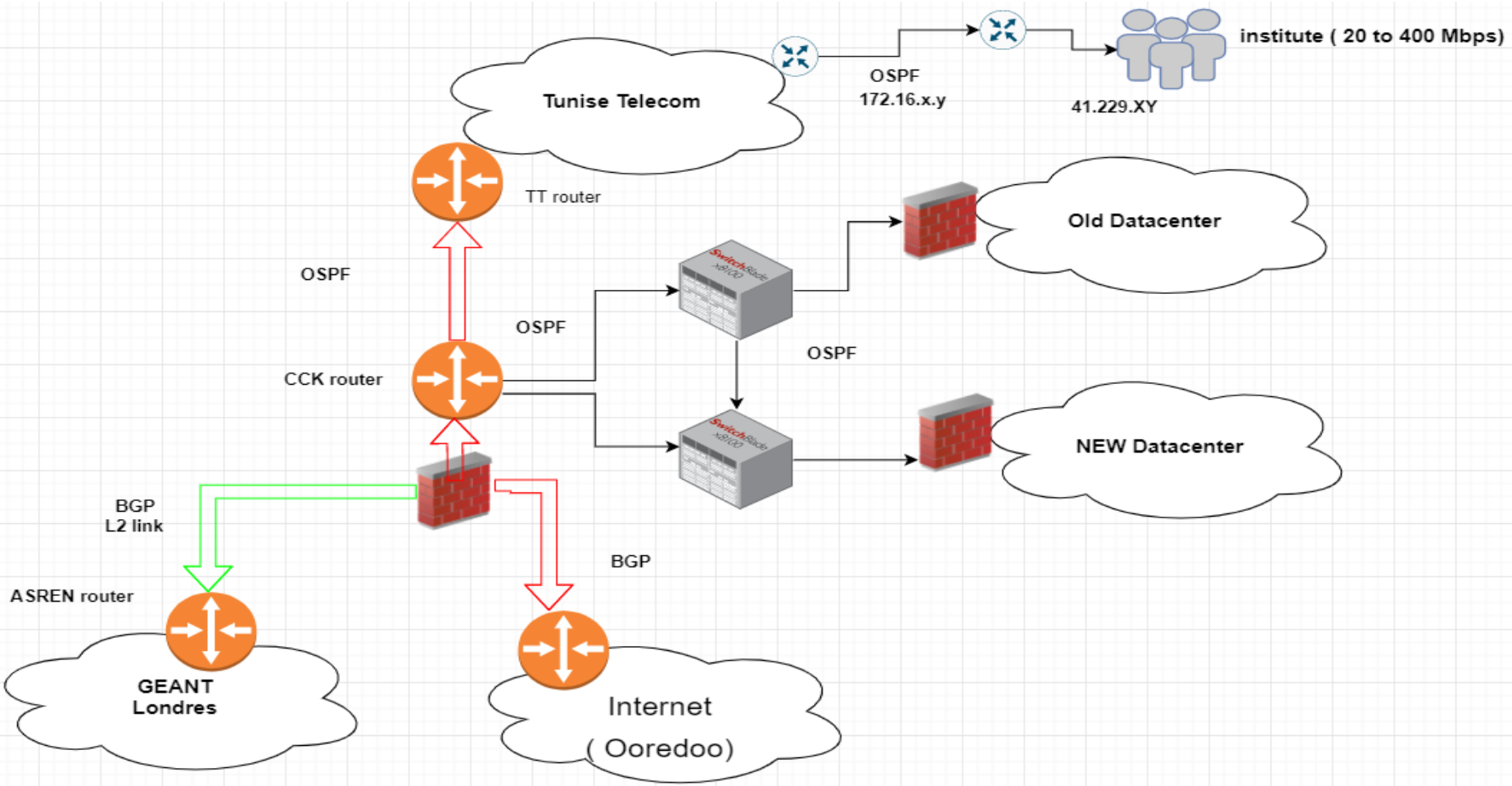


Réseau National Universitaire RNU4



2021 Core RNU Topology

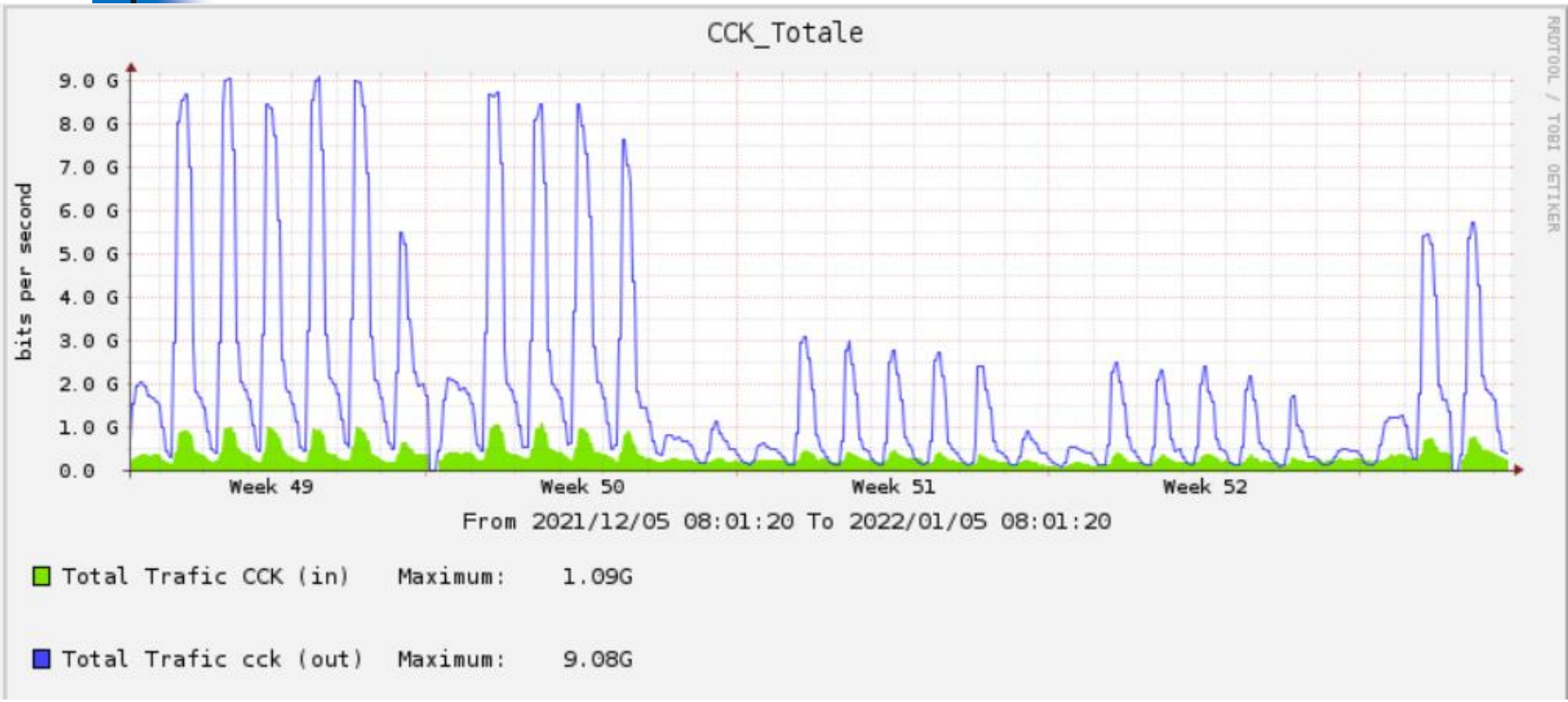
Peering PoP Mannouba 2022



Réseau National Universitaire 4 (2021)

Débits	Nombre des sites	Contrat SLA-Opérateur: Classe de service
10 Mbps	24	Silver
20 Mbps	92	Silver
30 Mbps	80	Silver
50 Mbps	110	Silver
70 Mbps	61	Silver
100 Mbps	92	Silver
150 Mbps	20	Silver
200 Mbps	15	Silver
300 Mbps	7	Silver
400 Mbps	6	Silver
Nombre des sites	**507**	
Total Débits des EERs	**34 G**	
Débits des POP CCK	**Nombre des sites**	**Contrat SLA-Opérateur: Classe de service**
1 Gbps	20	Silver
20 Gbps PoP La Manouba	1	Diamond
20 Gbps PoP El-Manar	1	Diamond

Trafic sortant et entrant du RNU



La Bande passante consommée est de l'ordre de 9 Gbps

Avec un coût de 0,4 millions de dinars par an

Infrastructure

- Infrastructure Réseau
  - Réseau tout en fibre
  - Backbone de capacité 20 Gbps
  - Accès Internet de 20 Gbps
  - Deux Peering PoP dans les locaux du CCK (Mannouba et Manar)
  - Deux datacenter hautement disponible à Mannouba et prochainement à El-Manar
  - Connexion au réseau GEANT via ASREN

Infrastructure

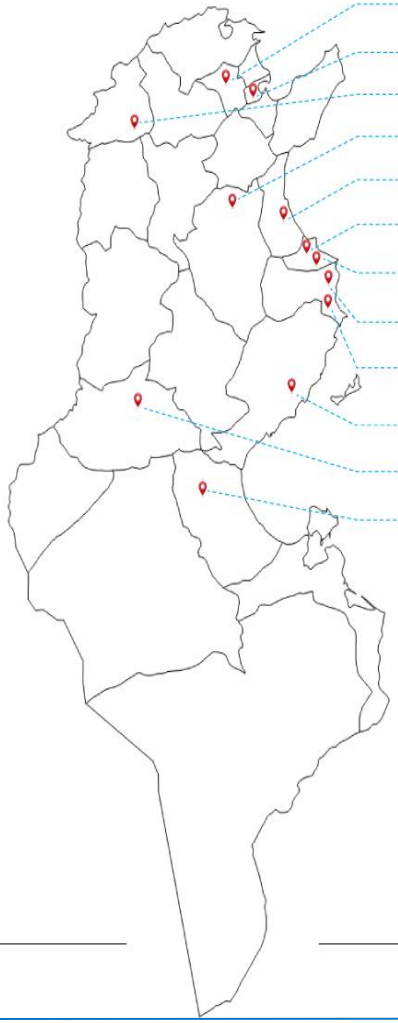
- Infrastructure Réseau
  - La mise en place de réseaux des campus (12 campus qui contient 90 établissements) et couvert par WiFi 6 (projet en phase de publication)
  - Rationalisation de la bande passante
  - La mise en place du protocole IPv6 dans le Réseau National Universitaire.

Réseaux des campus

12 CAMPUS UNIVERSITAIRES

120 ÉTABLISSEMENTS UNIVERSITAIRES

- Connexion FO
- Couverture Wifi6
- Aspect Sécurité



- Campus Manouba / 15 établissements
- Campus El-Manar / 7 établissements
- Campus de jendouba / 6 établissements
- Campus de kairouan / 6 établissements
- Campus de Sousse / 6 établissements
- Campus de Monastir / 6 établissements
- Campus de Monastir / 9 établissements
- Campus de Mahdia / 4 établissements
- Campus de Mahdia / 4 établissements
- Campus de Sfax / 10 établissements
- Campus de Gafsa / 4 établissements
- Campus de Gabès / 11 établissements

Infrastructure

- L’accés vers les applications nationales hébergées au CNI (ADAB, ELLISA, INSAF, etc) via des solutions VPN

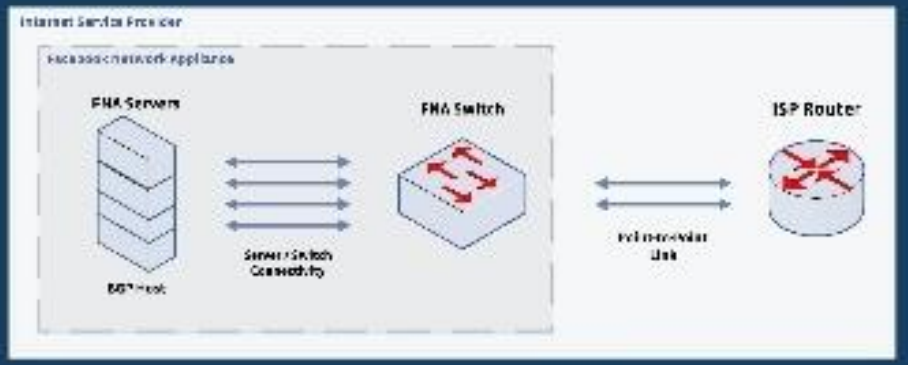
- Infrastructure sécurité
  - Sécurisation de l’RNU par des NG-Firewall
  - Solution Antiviral à la disposition des RNU
  - Des solution VPN (SSL et IPSEC).
  - WAF, LB

Facebook cache

FNA Deployments

Tech Specs

- Servers and Top of Rack Switch
- AC or DC Power
- Multiple 10GE or 100GE Uplinks



Considerations

- Peak Traffic
- Distance to Nearest PoP
- Latency and Application Performance
- Growth Rate of Market

Monitoring et supervision

- Supervision et notification avant incident : même par SMS
  - Réseaux (NOC)
  - Serveurs
  - Applications
  - Base de données
  - Environnement du data center
  - SOC (en cours de préparation)
- Outil d'aide pour diagnostique après incidents pour s'en prévenir prochainement

Formation: CCK-training-Center

http://www.cck.rnu.tn/training/

Cycle 1 :

- session 1 *du 03 au 05 Avril 2018.*
- session 2 *du 24 au 26 Avril 2018.*
- session 3 *du 02 au 04 Mai 2018.*
- session 4 *du 08 au 10 Mai 2018.*
- session 5 *du 03 au 05 Juillet 2018.*
- session 6 *du 16 au 18 Octobre 2018*

Ces cycles de formation ont pour thème principal la structuration et la sécurisation du réseau informatique d'un établissement universitaire

Formation: CCK-training-Center

http://www.cck.rnu.tn/training/

Cycle 2 :

- Session 1 du 03 au 05 Septembre 2019.
- Session 2 du 01 au 03 Octobre 2019.
- Session 3 du 26 au 28 Novembre 2019.
- Session 4 du 15 au 17 Janvier 2020.
- Session 5 du 25 au 27 Février 2020.

Thème: Structurer et sécuriser le réseau Informatique d'un établissement universitaire : Travaux Pratiques, Niveau Avancé

Gouvernance / NORME

- Agir en faveur d'un meilleur positionnement du CCK dans le milieu académique
- Adopter une Gouvernance centrée qualité à tous les niveaux
  - Le CCK a lancé un appel d'offre pour l'accompagnement à la certification ISO 27001 (ISMS)
  - Etre à l'écoute de nos clients en vue d'aligner nos services à leurs besoins et attentes

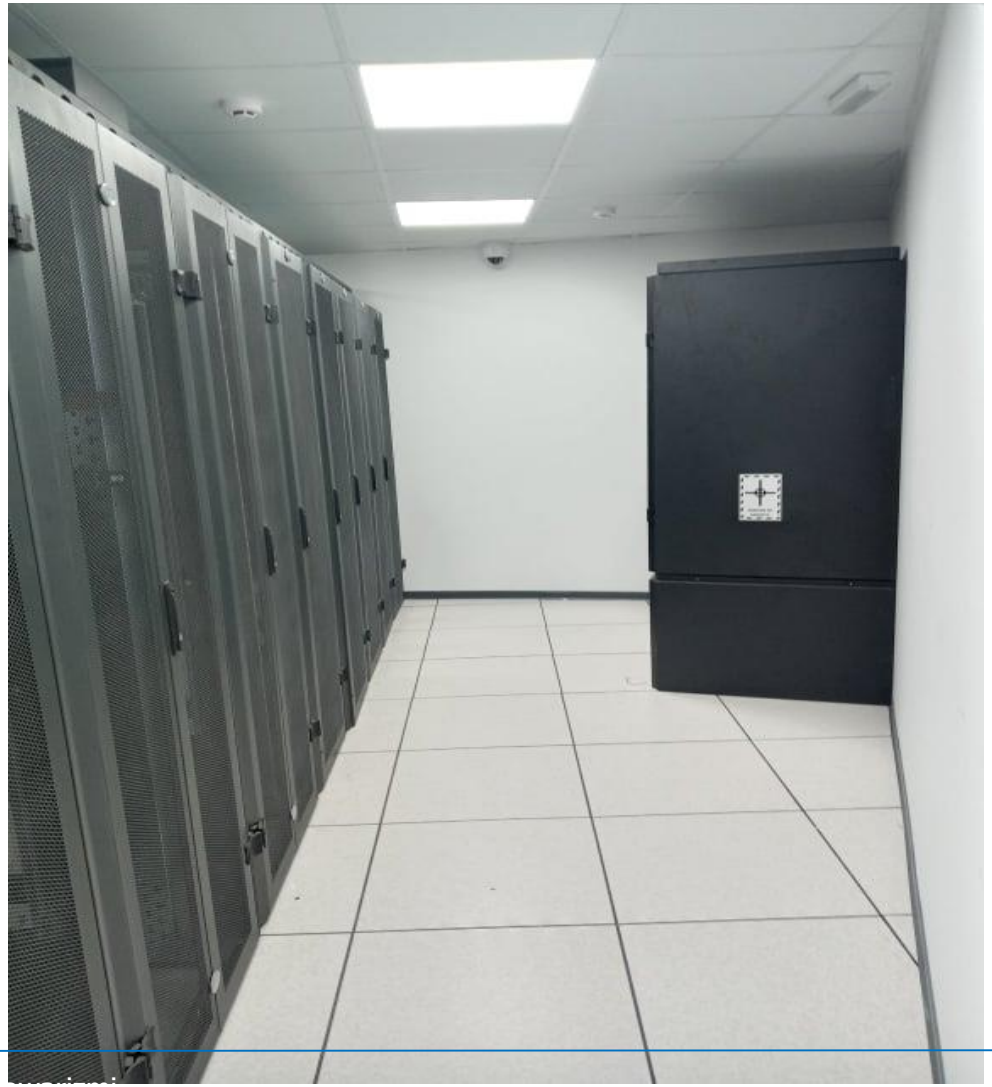
Caractéristiques du Nouveau Datacenter

- Site de Production: DATA CENTER Manouba
  - 16 armoires 42 U
    - Armoires ondulées
    - Câblage préconnectorisé Fibre et Rj45
    - CONFINNEMENT COULOIR FROID
    - Deux PDU provenant de deux sources d'alimentation différents
    - Groupe électrogène
    - SECURITE physique et contrôle d'accès:

    (Vidéosurveillance, Détection et Extinction Incendie, Contrôle d'accès)
    - GENIE CIVIL (Faux plancher, Dalles perforées, Plaque de plâtre coupe feu, portes coupe feu)
- Site de Secours: DATA CENTER Manar
  - En Phase d'exécution (Aménagement)

Datacenter CCK: photo de la Salle IT

Salle IT: Climatisation de précision



Salle d’énergie: Armoires Electriques, Onduleurs, Eclairages

CCK 2020: **Mise en place du nouveau Datacenter : Les équipements Actifs**

Des équipements Réseau

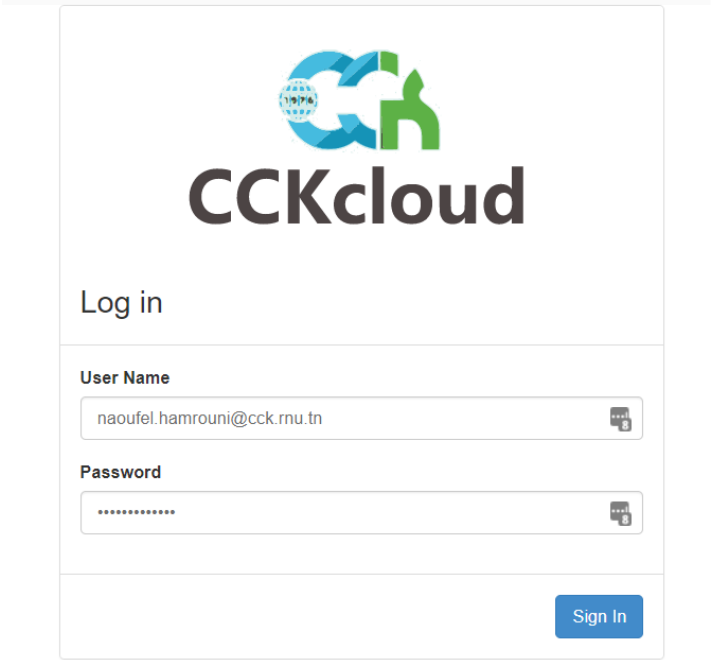
- Core Switch (actif/Passif)
- Switch d'agrégation (Actif/Actif)

Des équipements de sécurité

- Firewalls (actif/actif)
- IPS : Intrusion prevention system (actif/actif)
- WAF (actif/actif)
- solution VPN SSL
- répartiteurs de charges (actif/passif)

Présentation de la plateforme

https://console.cckcloud.rnu.tn/



openstack.

OPENSHIFT by Red Hat

Terraform

Présentation de la plateforme

- Solution à base **Openstack** et **Ceph**.
- Dernières Versions Stables.
- Déploiement automatisé.
- Architecture avec Haute disponibilité.
- Multi-zones.
- Monitoring de la plateforme avec Grafana.

Présentation de la plateforme

Architecture:

3 Controllers

openstack

9 Computes (Zone CCK)

ceph

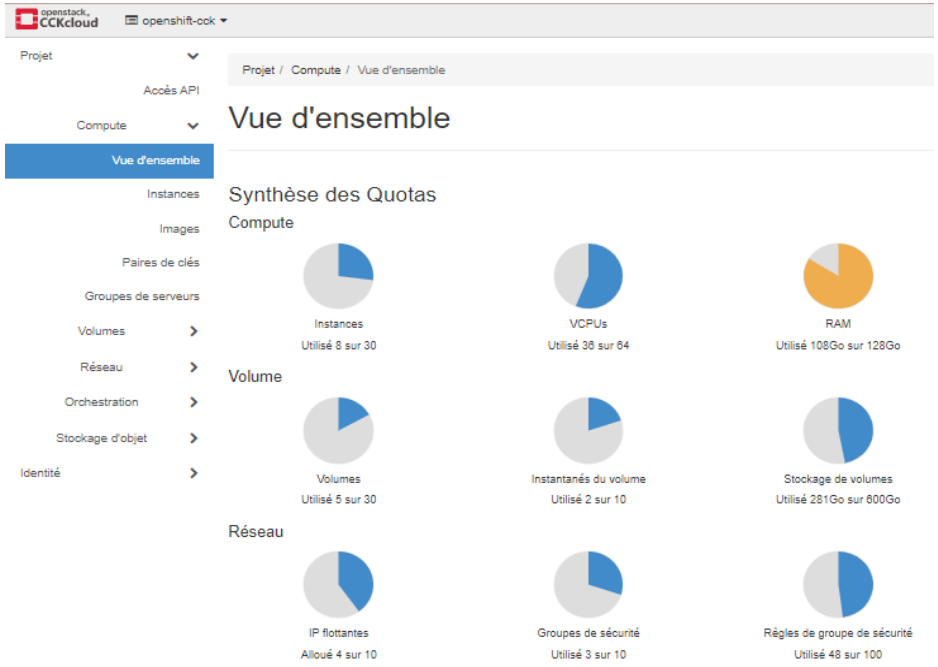
3 Nœuds Object Storage

Baie de stockage

Connectivité: Liens de 10Gb Ethernet et 16Gb FC

Présentation de la plateforme

Panneau de contrôle:



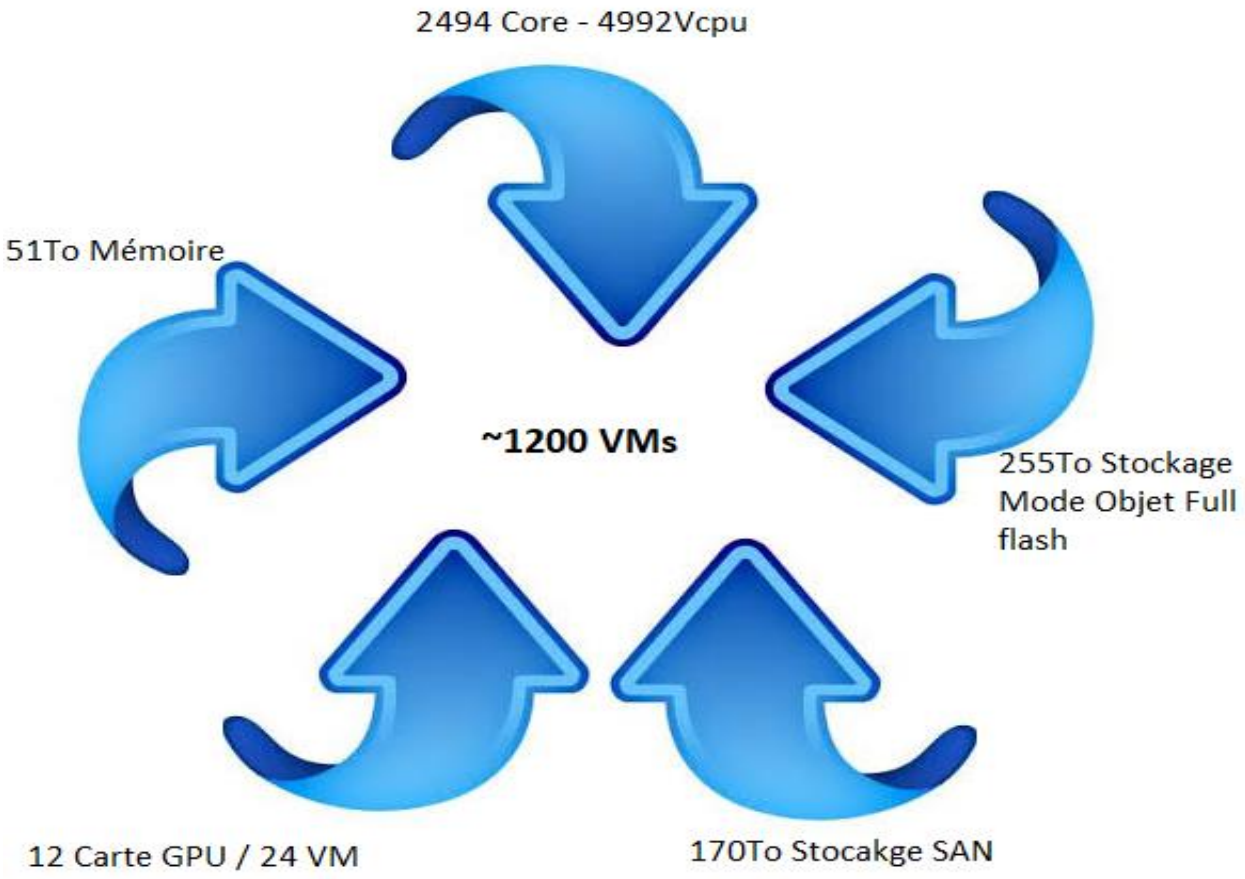
- **720** vcpu
- **6,7 To** mémoire
- **100To** stockage SSD/SAS
- Bande passante de **10 Gbs**
- **510** @ipv4 Publique

Présentation de la plateforme

Services:

- IaaS : **OK**
- LBaaS **OK**
- VPNaaS En cours
- DBaaS Prochainement
- PaaS: Openshift En cours

Ressources


2494 Core - 4992Vcpu
51To Mémoire
~1200 VMs
255To Stockage Mode Objet Full flash
12 Carte GPU / 24 VM
170To Stocakge SAN

openstack

ceph

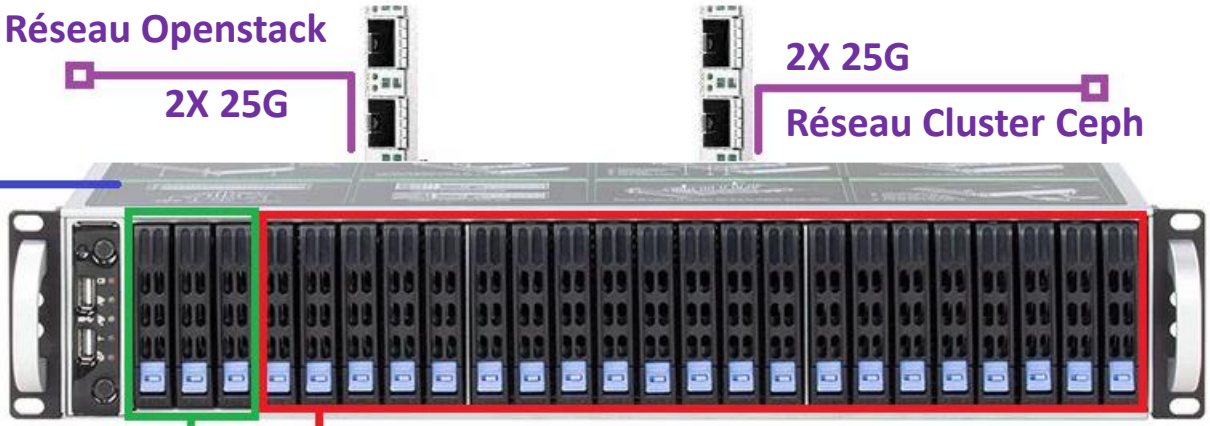
48 Lames : 2X 25Go / Lame avec bande passante au total de 2400Go

Nous prévoyons l'extension jusqu'à 4 châssis de plus, sans provisionnement supplémentaire du réseau en uplink.

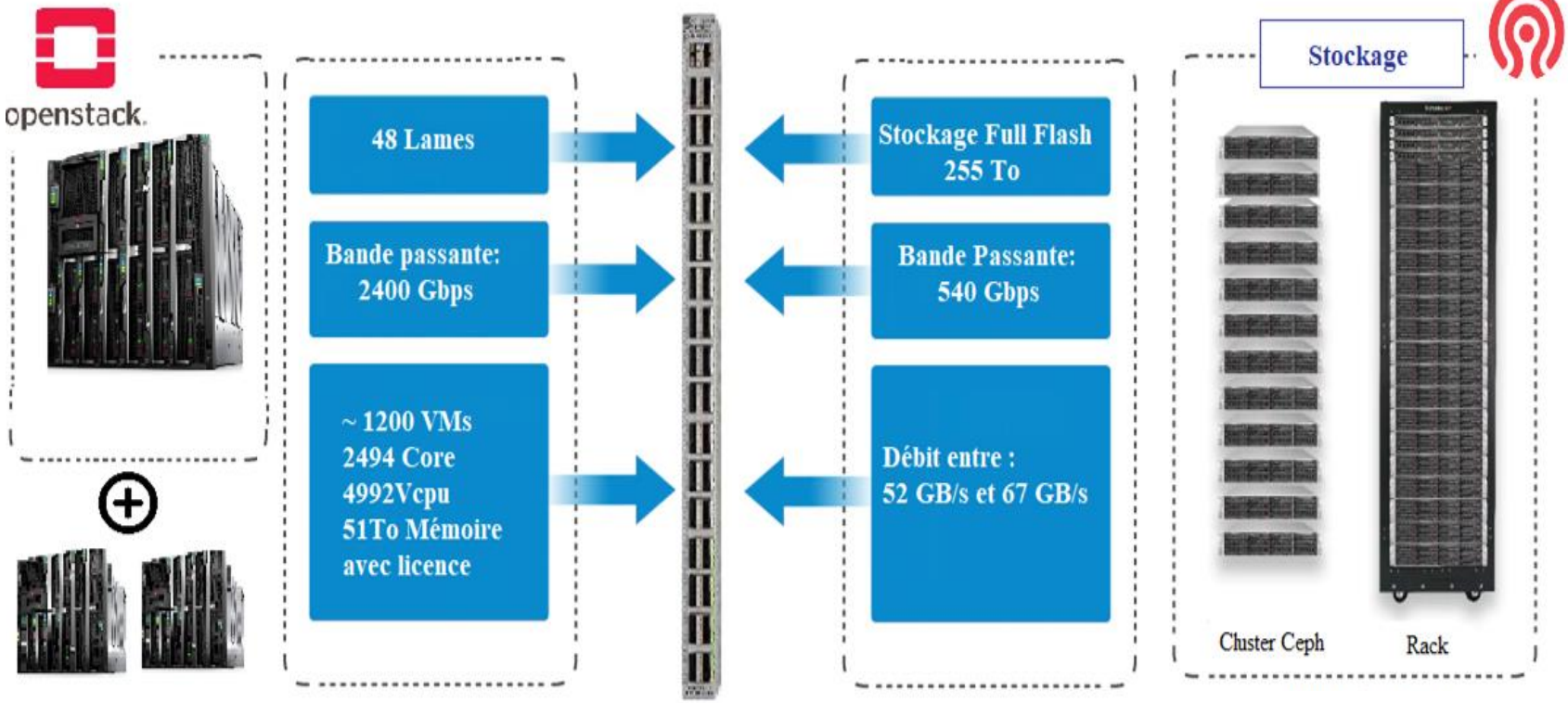
- **12 Nœuds Rack**
- **Bande passante estimée entre 420Go et 540Go selon la vitesse du disque SSD**
- **Séquentiel: Débits Max total: 67Go/s vers Openstack**
- **Aléatoire : débit Max Total : 24Go/s vers Openstack**
- **Réplication 3, coefficient de sécurité 0,8**

Possibilité d'étendre le cluster Ceph jusqu'à 12 Nœuds de plus, pour passer à 1080Go.

ceph


Réseau Openstack
2X 25G
2X 25G
Réseau Cluster Ceph
2 Disk M2/SSD
Système OS
BlueStore Journal
3 Disk NVME 1,92To
OSD (data)
21 Disk SSD SATA 3,98To

X12



Plateforme Computing

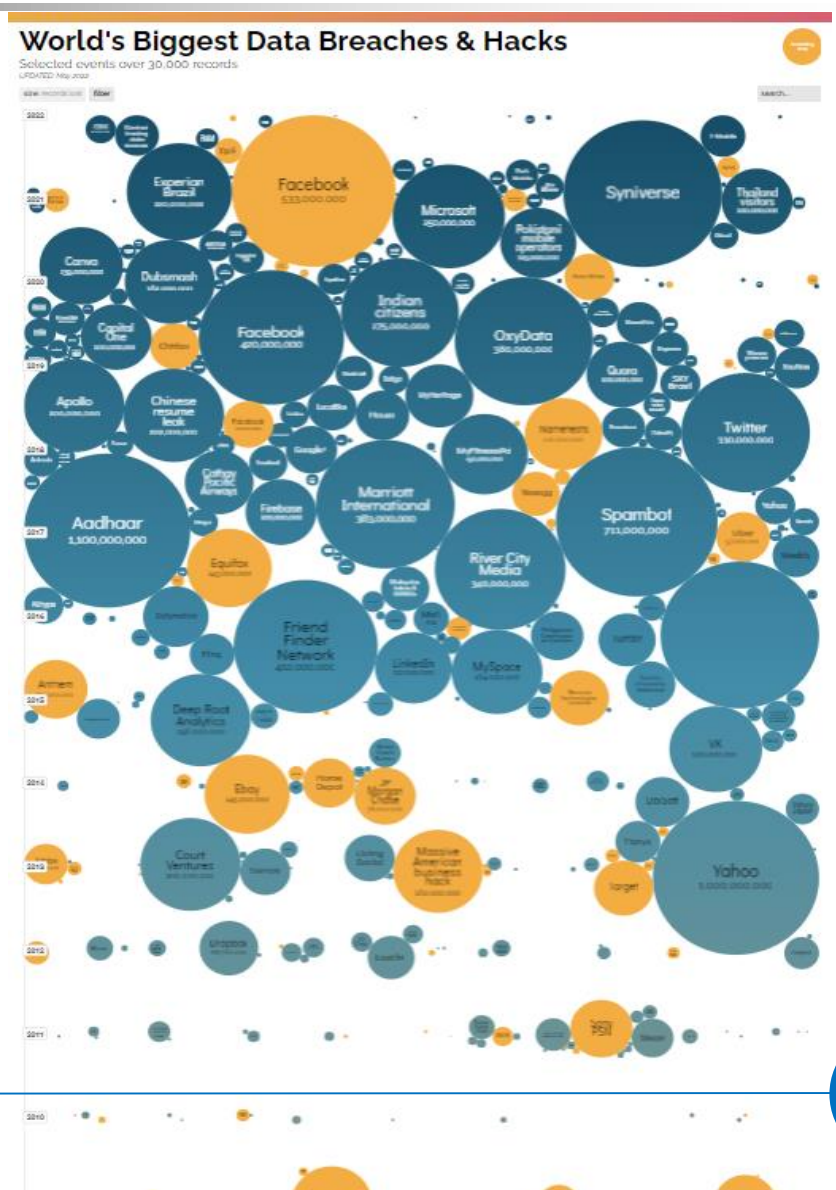
Plateforme Ceph

Connectivité norme standard

- On va passer de 10Gb à 25Gb pour Ethernet, de 16Gb à 32Gb pour FC
- Ports de 100Go
- Technologie Spine and Leaf pour le switching.

Les challenges de sécurité

- Cyber crime est un risque commun à tous et son impact devient de plus en plus important. Le nombre d'attaques augmente de **10%** chaque année et son coût aussi augmente d'une manière considérable .



Les challenges de sécurité

- Les attaques prennent quelques minutes pour être concrétisées, mais plusieurs jours pour être détectées (211 jours) et plusieurs autres jours pour être supprimées (54 jours).
- La composante cloud (privé, public et hybride) a ajouté plus de chalenge en terme de sécurité.
- 80% du trafic est crypté (Encrypted Malware)

Les challenges de sécurité

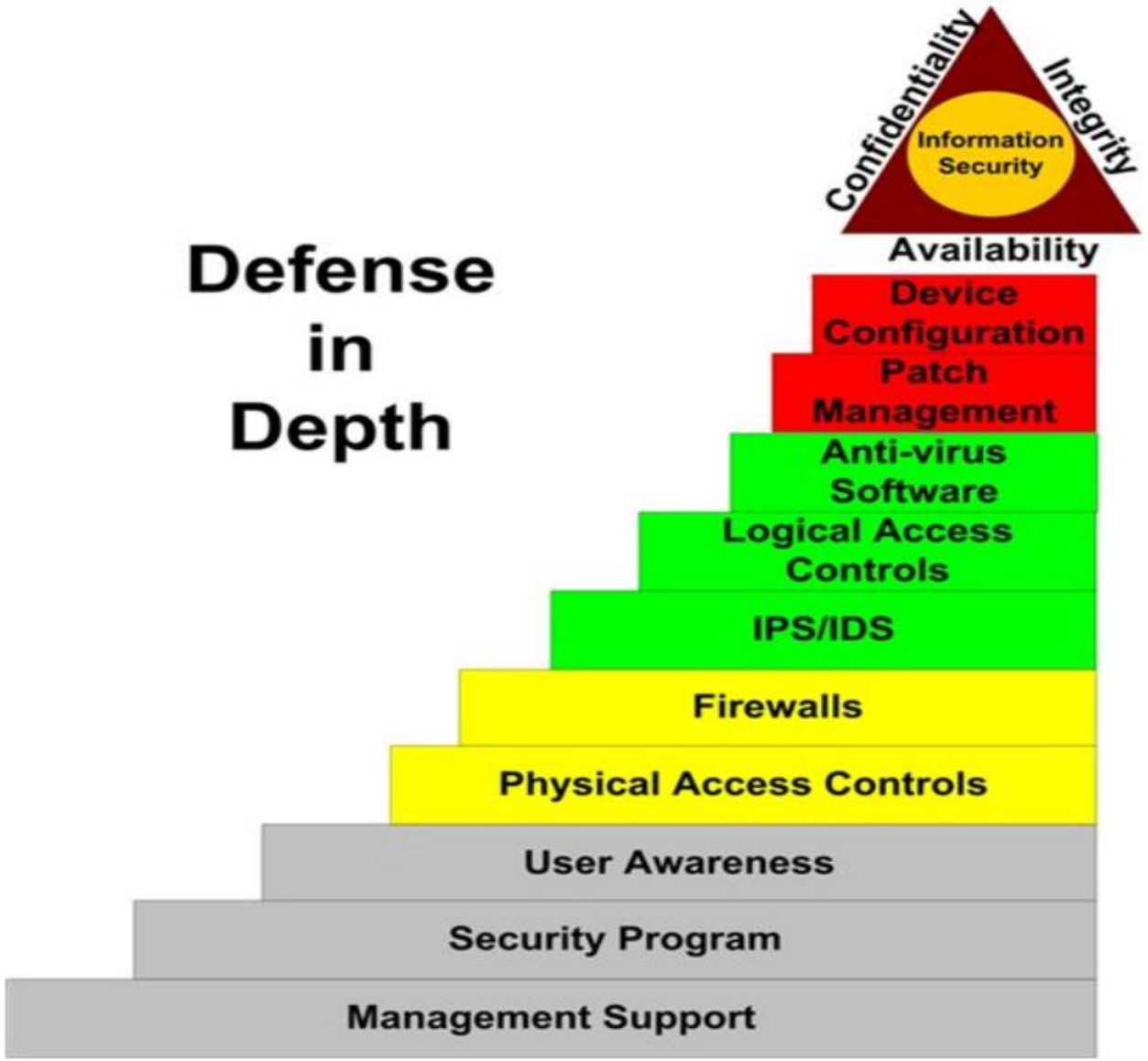
- Les changements rapides des équipements de sécurité et des réseaux pour remédier au changement rapide dû aux nouvelles menaces (thred).

Les challenges de sécurité

- Chaque société contient plusieurs équipements de sécurité, mais le problème et au niveau de la communication entre ces equipments de securite.
- Les résistance au changement des employés et le choix d'utiliser les mêmes équipements ou le même constructeur au lieu d'apprendre de nouvelles connaissances.

Les challenges de sécurité

- Plus le réseau devient grand plus le chalenge en sécurité et de maitrise devient plus grand.
- Le challenge de maintenir un staff bien formé et compétant.
- Les architects reseau doivent prioriser la sécutité dans toutes les phases (planification, mise en place et exploitation).



https://www.brighthub.com/computing/smb-security/articles/2217/

pfSense

pfSense peut jouer le rôle d’ :

1. Un Portail Captive
2. Proxy
3. concentrateur VPN
4. IDS/IPS
5. Traffic Shaping
6. analyseur de trafic
7. Serveur Radius
8. Autorité de certification CA
9. autres

ADMINISTRATION de pfSense

Configuration

- Web-based configuration
- Setup wizard for initial configuration
- Remote web-based administration
- Customizable dashboard
- Easy configuration backup/restore
- Configuration export/import
- Encrypted automatic backup to Netgate server
- Variable level administrative rights
- Multi-language support
- Simple updates
- Forward-compatible configuration
- Serial console for shell access and recovery options

System Security

- Web interface security protection
- CSRF protection
- HTTP Referer enforcement
- DNS Rebinding protection
- HTTP Strict Transport Security
- Frame protection
- Optional key-based SSH access

Reporting & Monitoring

- Dashboard with configurable widgets
- Local logging
- Remote logging
- Local monitoring graphs
- Real-time interface traffic graphs
- SNMP monitoring
- Notifications via web interface, SMTP, or Growl
- Hardware monitoring
- Networking diagnostic tools

Quelques fonctionnalités de pfSense

Firewall and Router

- Stateful Packet Inspection (SPI)
- GeoIP blocking
- Anti-Spoofing
- Time based rules
- Connection limits
- Dynamic DNS
- Reverse proxy
- Captive portal guest network
- Supports concurrent IPv4 and IPv6
- NAT mapping (inbound/outbound)
- VLAN support (802.1q)
- Configurable static routing
- IPv6 network prefix translation
- IPv6 router advertisements
- Multiple IP addresses per interface
- DHCP server
- DNS forwarding
- Wake-on-LAN

VPN

- IPsec and OpenVPN
- Site-to-site and remote access VPN support
- SSL encryption
- VPN client for multiple operating systems
- L2TP/IPsec for mobile devices
- Multi-WAN for failover
- IPv6 support
- Split tunneling
- Multiple tunnels
- VPN tunnel failover
- NAT support
- Automatic or custom routing
- Local user authentication or RADIUS/LDAP

Intrusion Prevention System

- Snort-based packet analyzer
- Layer 7 application detection
- Multiple rules sources and categories
- Emerging threats database
- IP blacklist database
- Pre-set rule profiles
- Per-interface configuration
- Suppressing false positive alerts
- Deep Packet Inspection (DPI)
- Optional open-source packages for application blocking

Quelques fonctionnalités de pfSense

Enterprise Reliability

- Optional multi-node High Availability Clustering
- Multi-WAN load balancing
- Automatic connection failover
- Bandwidth throttling
- Traffic shaping wizard
- Reserve or restrict bandwidth based on traffic priority
- Fair sharing bandwidth
- User data transfer quotas

User Authentication

- Local user and group database
- User and group-based privileges
- Optional automatic account expiration
- External RADIUS authentication
- Automatic lockout after repeated attempts

Proxy and Content Filtering

- HTTP and HTTPS proxy
- Non Transparent or Transparent caching proxy
- Domain/URL filtering
- Anti-virus filtering
- SafeSearch for search engines
- HTTPS URL and content screening
- Website access reporting
- Domain Name blacklisting (DNSBL)
- Usage reporting for daily, monthly, etc.

Les ressources du pfSense

General Requirements:	
Minimum	• CPU - 500 Mhz • RAM - 512 MB
Recommended	• CPU - 1 Ghz • RAM - 1 GB
Requirements Specific to Individual Platforms:	
Full Install	• CD-ROM or USB for initial installation • 1 GB hard drive

Recommandations pour sécuriser

- Activer uniquement les services de management utiles : n'utiliser que les protocoles sécurisés (ssh, https).
- Désactiver les ports qui ne sont pas utilisés.
- Réaffecter les ports du Vlan par défaut à un Vlan non utilisable dans votre réseau.
- Utiliser des mots de passe robustes et les changer périodiquement.
- Crypter et ou hasher les mots de passe.

Recommandations pour sécuriser

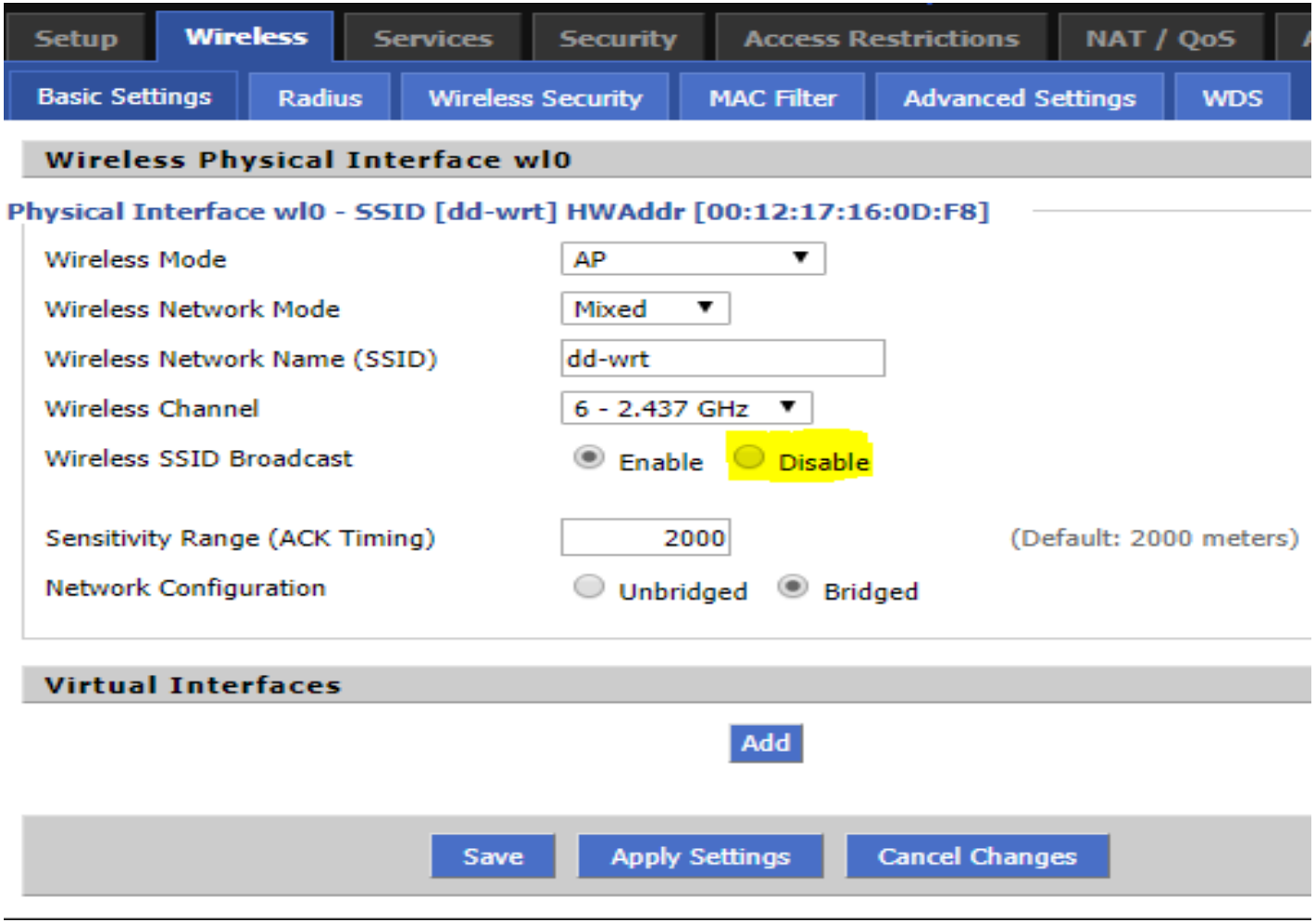
- Utiliser des ACL
- Utiliser des Bannières dissuasives.
- Utiliser les DHCP snooping pour arrêter les attaques de type rogue DHCP server.
- Activer les “ports security” pour arrêter les attaques de type MAC flooding au DHCP starvation.
- Désactiver le CDP et LLDP .
- Utiliser 802.1x pour authentifier l’accès au LAN

Recommandations pour sécuriser

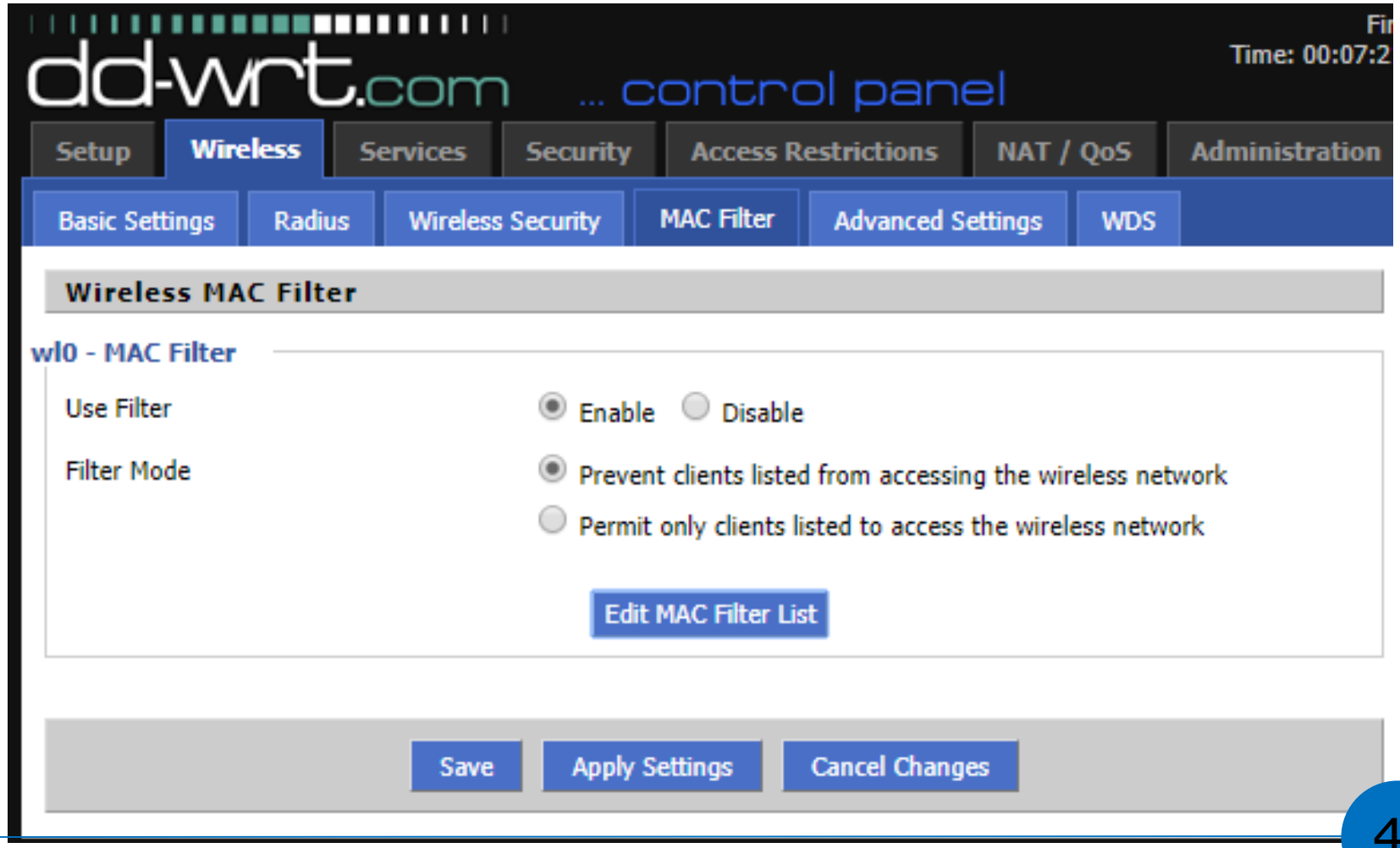
- Dynamic ARP Inspection (DAI) pour arrêter les attaques de type MITM, ARP spoofing, MAC flooding, etc
- Protéger l'architecture spanning tree en applicant BPDU Guard, BPDU Filter et Root Guard
- Ne pas laisser les ports en mode auto négociation pour arrêter les attaques de type VLAN hopping.
- Ne pas laisser les ports affectés au Vlan par défaut (Vlan 1).

quelque mesure de sécurité pour les réseaux WLAN

Cacher l'SSID du réseau

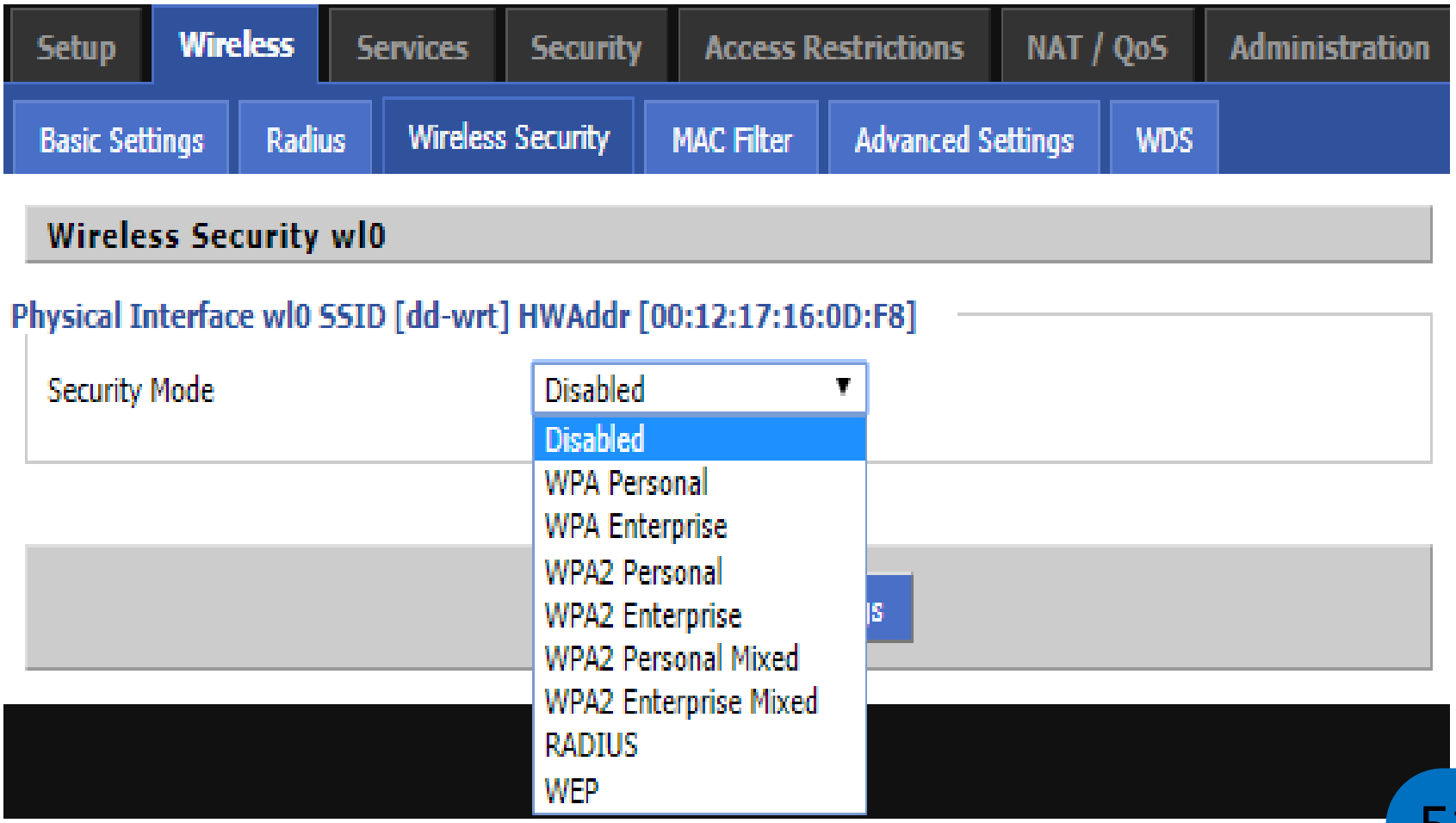


Filtrage des MAC autoriser



Pre-shared key

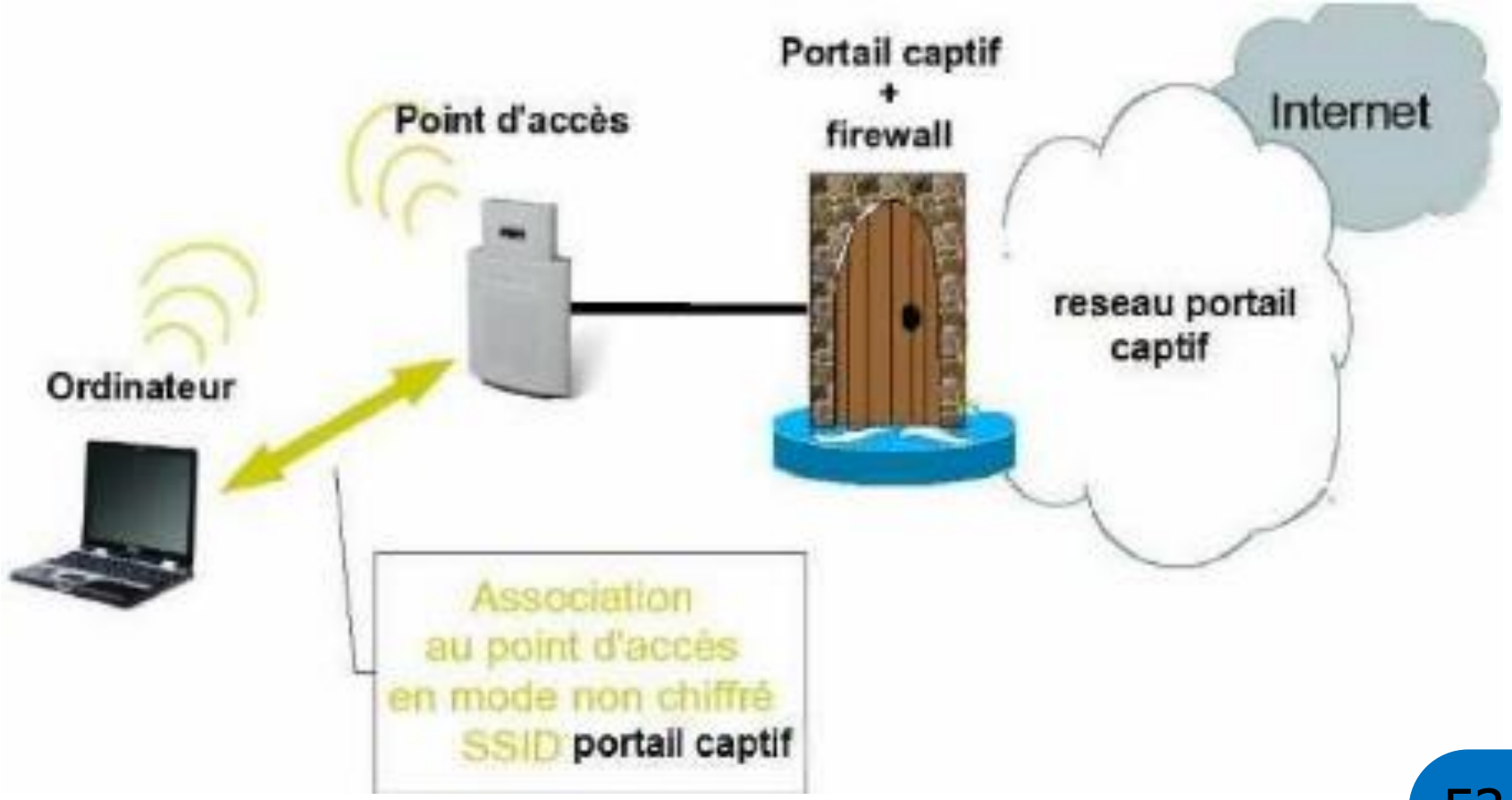
https://www.cyberpunk.rs/wireless-security-protocols-wep-wpa-wpa2-and-wpa3.html


Setup
Wireless
Services
Security
Access Restrictions
NAT / QoS
Administration
Basic Settings
Radius
Wireless Security
MAC Filter
Advanced Settings
WDS
Wireless Security wl0
Physical Interface wl0 SSID [dd-wrt] HWAddr [00:12:17:16:0D:F8]
Security Mode
Disabled
Disabled
WPA Personal
WPA Enterprise
WPA2 Personal
WPA2 Enterprise
WPA2 Personal Mixed
WPA2 Enterprise Mixed
RADIUS
WEP

Besoin d'un contrôleur Wi-Fi

- Pour gérer facilement plusieurs AP installés dans un établissement, un contrôleur Wifi est utile pour.
  - Gérer automatique des canaux radio
  - Configurer et administrer les divers points d'accès d'une façon centralisée, aisée par une GUI
  - En cas de disfonctionnement d'un AP particulier, il sert à augmenter la couverture du signal de ces AP voisins, pour assurer la couverture wifi
  - Statistiques et rapports
  - Sécurité

Service Portail Captif: Architecture



https://www.cyberpunk.rs/wireless-security-protocols-wep-wpa-wpa2-and-wpa3.html

Hotspot Portal

Sputnik

SPUTNIK®

Sputnik Agent — ○ Enable ● Disable

Hotspot System

HOTSPOTSYSTEM.com

Hotspot System — ○ Enable ● Disable

Wifidog

Wifidog
A captive portal suite

Wifidog daemon — ○ Enable ● Disable

Chillispot

Chillispot — ○ Enable ● Disable

Chillispot Local User Management

User List	
Username	Password

Add Remove

Questions