Ecole polytechnique fédérale de Lausanne

Projet de segmentation réseau informatique - 2018

Blaise Mucaria VPSI - EXINFR

Introduction

1. But / description du projet
2. Planning
3. Zone
4. Phase 2
5. Phase 3
6. Question/discussion

Fiche du projet de segmentation réseau informatique - 2018

Mandant
Philippe Morel - EXOP

Responsable :
Blaise MUCARIA - EXINFR

Stockage des docs :
smb://scxdata/CommunVPSI$/EXINFR/01_Projets/2018_VRF-Segmentation/

Segment(s) du projet : IT for IT

Objectifs du projet :
Objectifs : Mise en place de la segmentation du réseau de l'EPFL afin de répondre au point d'audit sécurité R1417

Livrables à la fin du projet : zones de sécurité, automate de migration

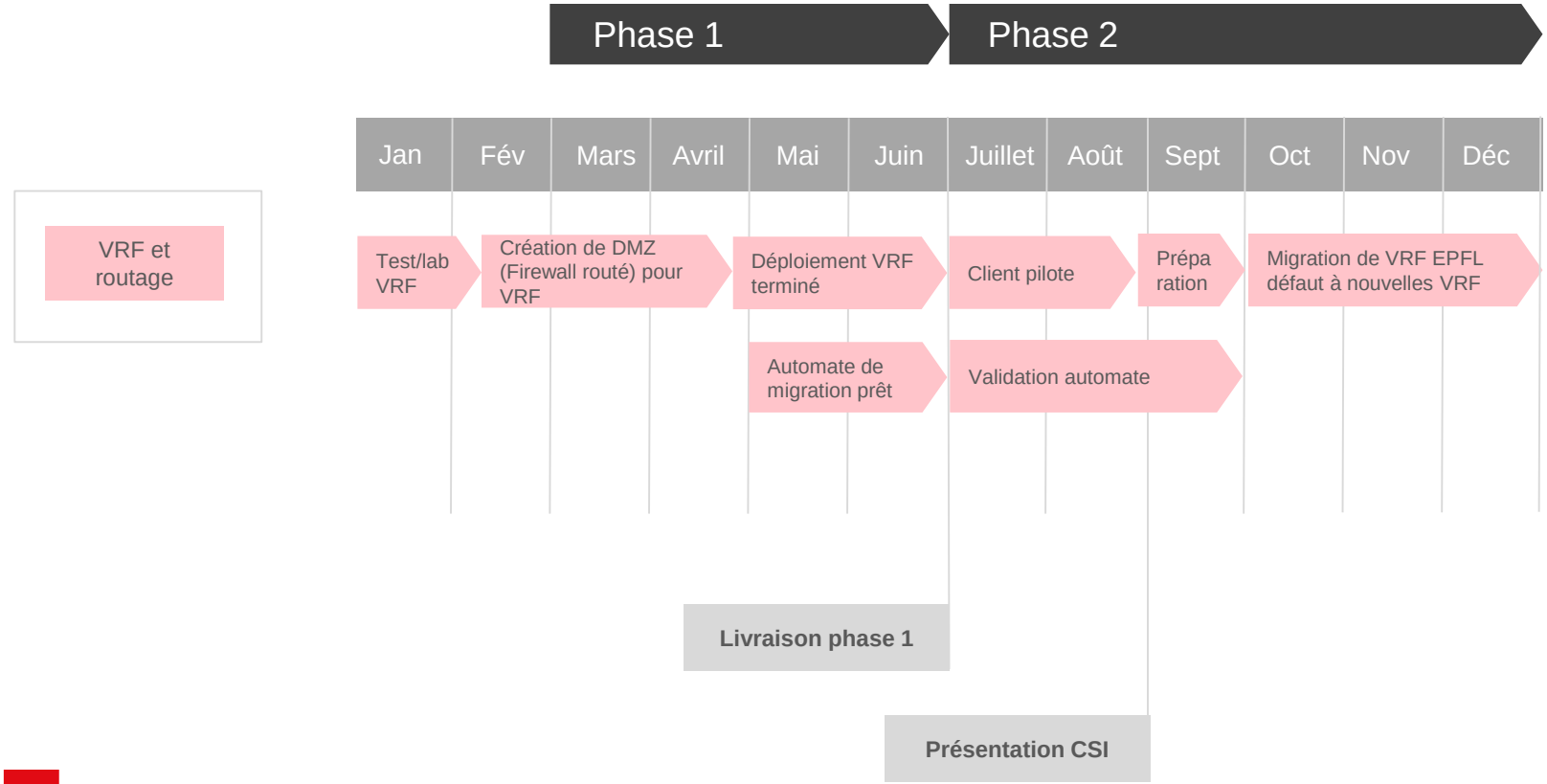
Parcipitants et rôles au projet :

- Nicolas Biselx - EXINFR - technique
- Julien Demierre - EXINFR - technique
- Philippe Gagnon - EXINFR - technique
- Daniel Grandjean - EXINFR - technique
- Jean-Luc Gugler - EXINFR – technique
- Jonathan Jaccard - EXINFR - technique
- Blaise Mucaria - EXINFR - Chef de projet
- Nicolas Repond - EXINFR - Automatisation / scriptes / Sécurité
- Jacques Rochat - EXINFR - technique
- Thierry Ruffieux - EXINFR - Architecte réseau
- Patrick Saladino - EXAPP - Sécurité
- Alexandre Sutlian - EXAPP - Sécurité
- Jean-François Dousson - GOUV-GE - Sécurité

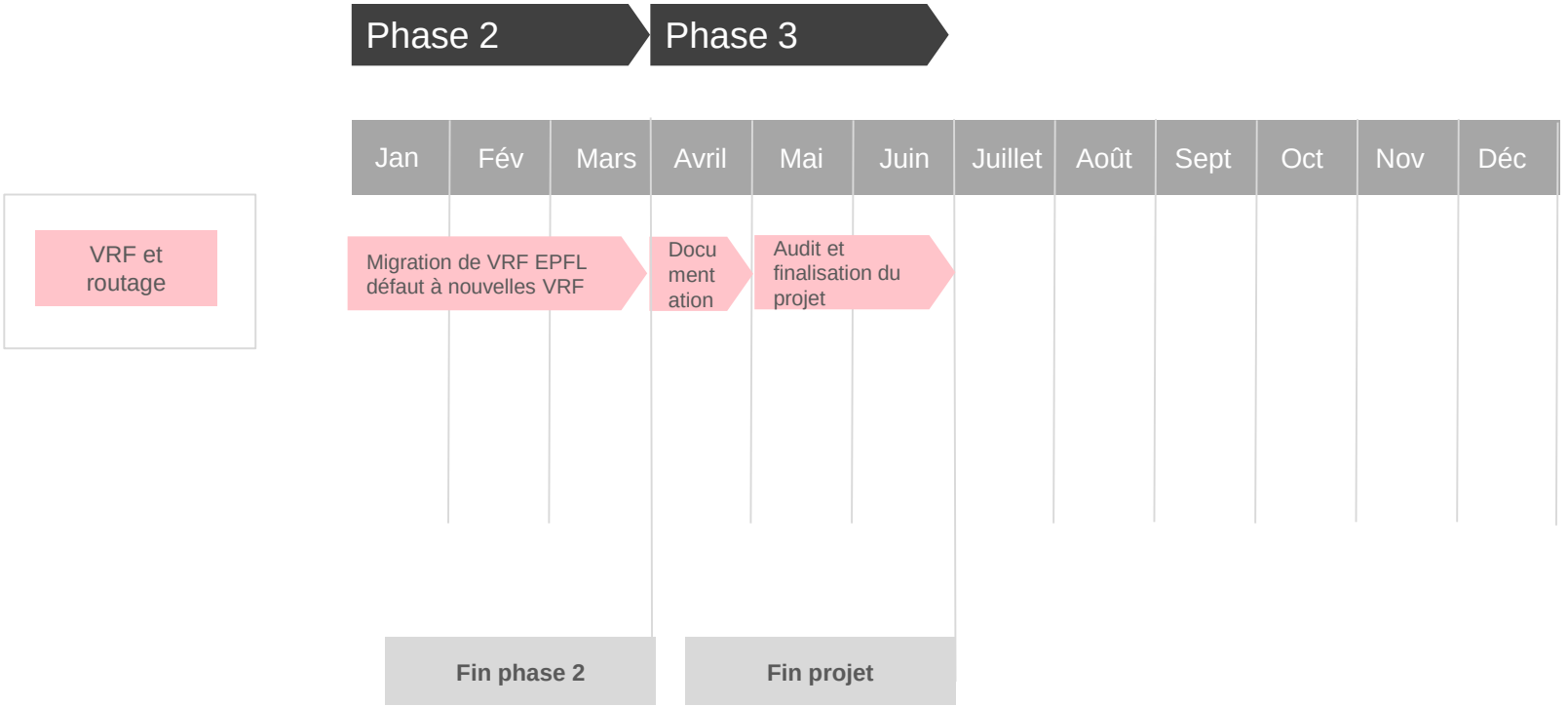
	Estimations initiales	
Investissement/CAPEX	0	(Investissement réalisé en 2014 - 2015)
Investissement/RH	200 Jours Homme	

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Planning 2018

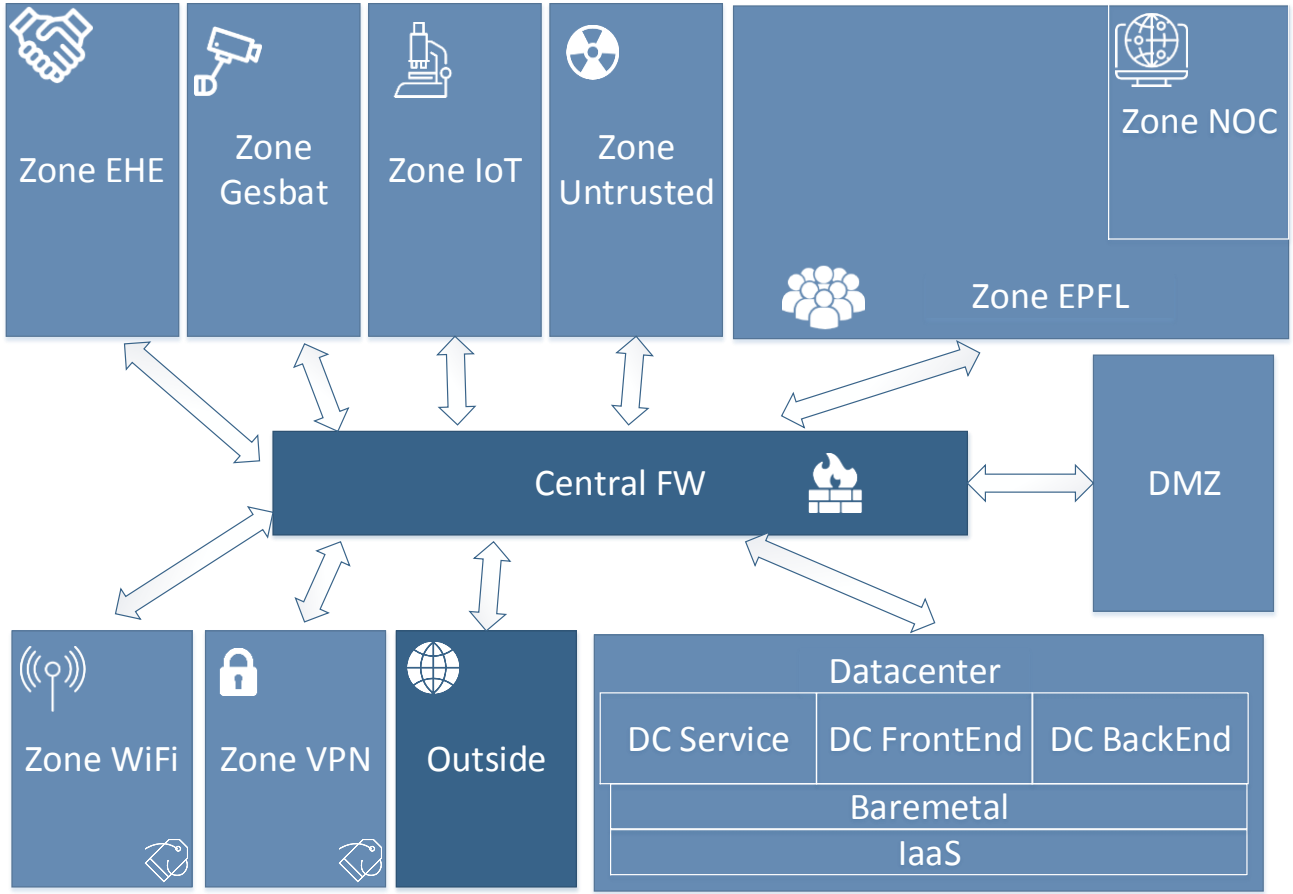


Planning 2019

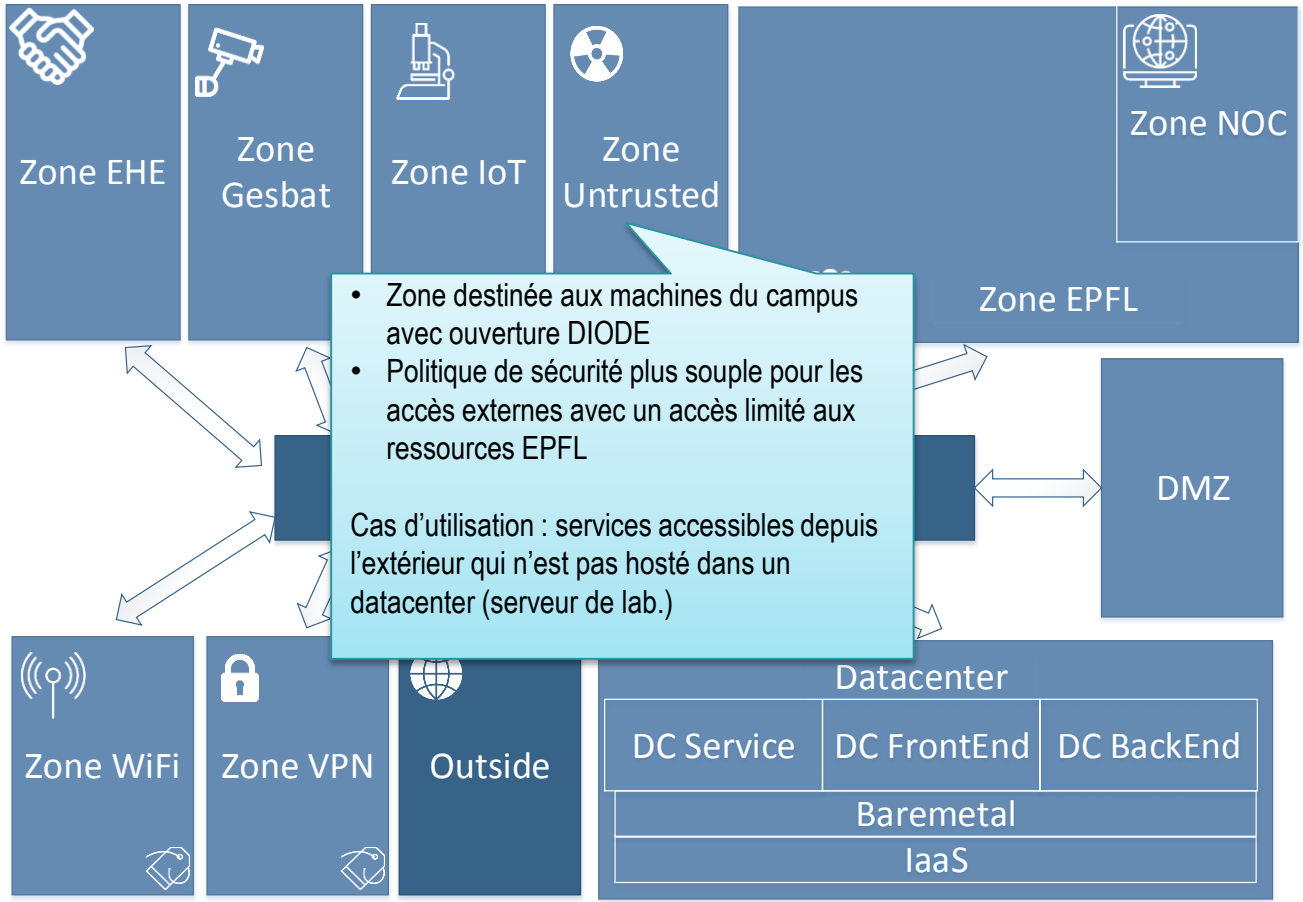


Zones

Présentation des zones



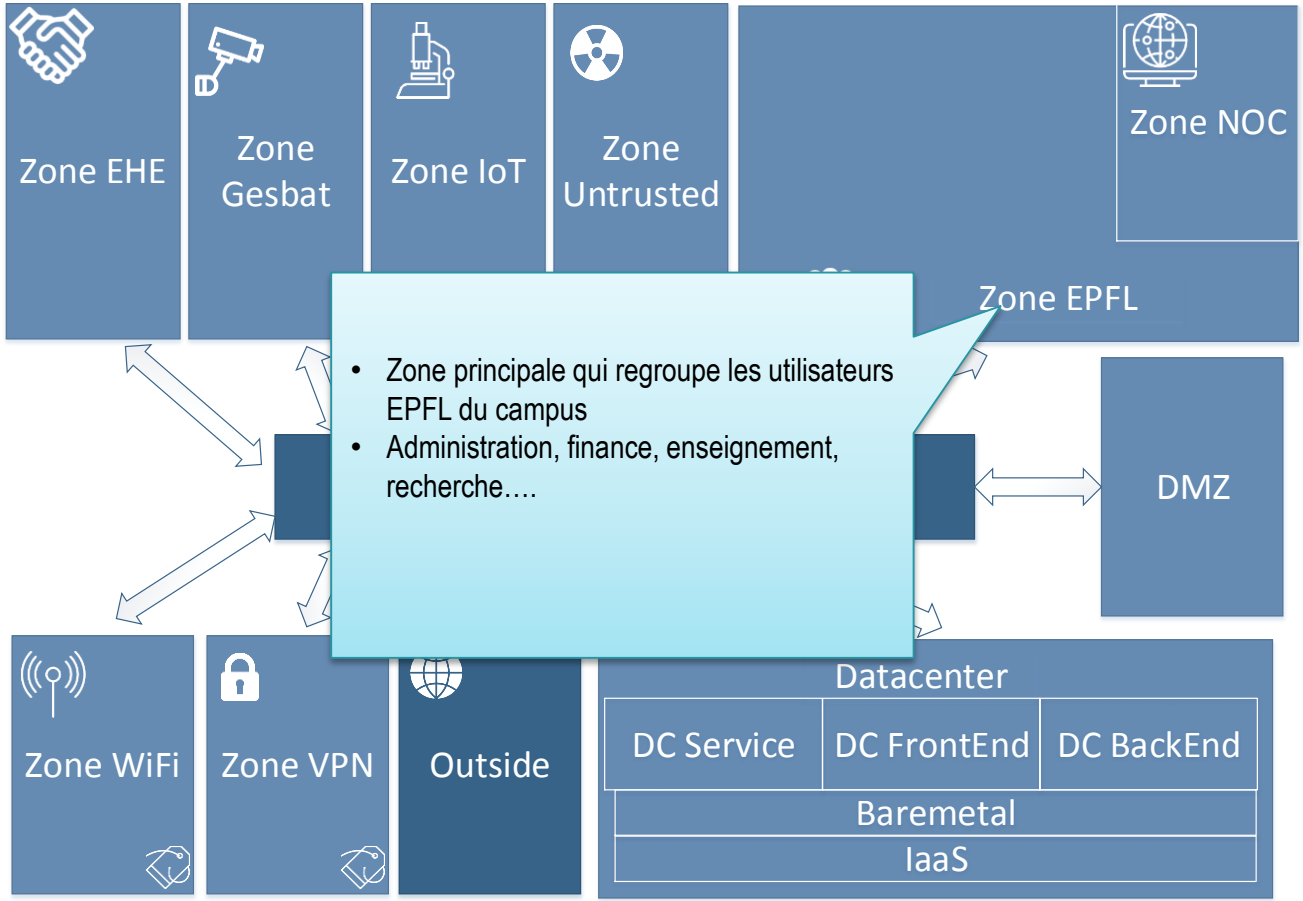
Présentation des zones



- Zone destinée aux machines du campus avec ouverture DIODE
- Politique de sécurité plus souple pour les accès externes avec un accès limité aux ressources EPFL

Cas d'utilisation : services accessibles depuis l'extérieur qui n'est pas hosté dans un datacenter (serveur de lab.)

Présentation des zones



- Zone principale qui regroupe les utilisateurs EPFL du campus
- Administration, finance, enseignement, recherche….

Matrice de sécurité pour la segmentation

(ref. Gouvernance du réseau IT)

Version 2.1

14.11.2018 BM

	Source	Destinations	Outside	DMZ	DC service	Zone Untrusted	Zone EHE	DC Frontend	Zone IoT	Zone Gesbat	Zone EPFL	Zone VPN	Zone Wifi	DC Backend	Zone Noc
1	Outside														
10	DMZ														
15	DC Service														
20	Zone Untrusted														
25	Zone EHE														
30	DC Frontend														
35	Zone IoT														
40	Zone Gesbat														
45	Zone EPFL														
50	Zone VPN														
55	Zone Wifi														
60	DC Backend														
100	Zone Noc														

Légende

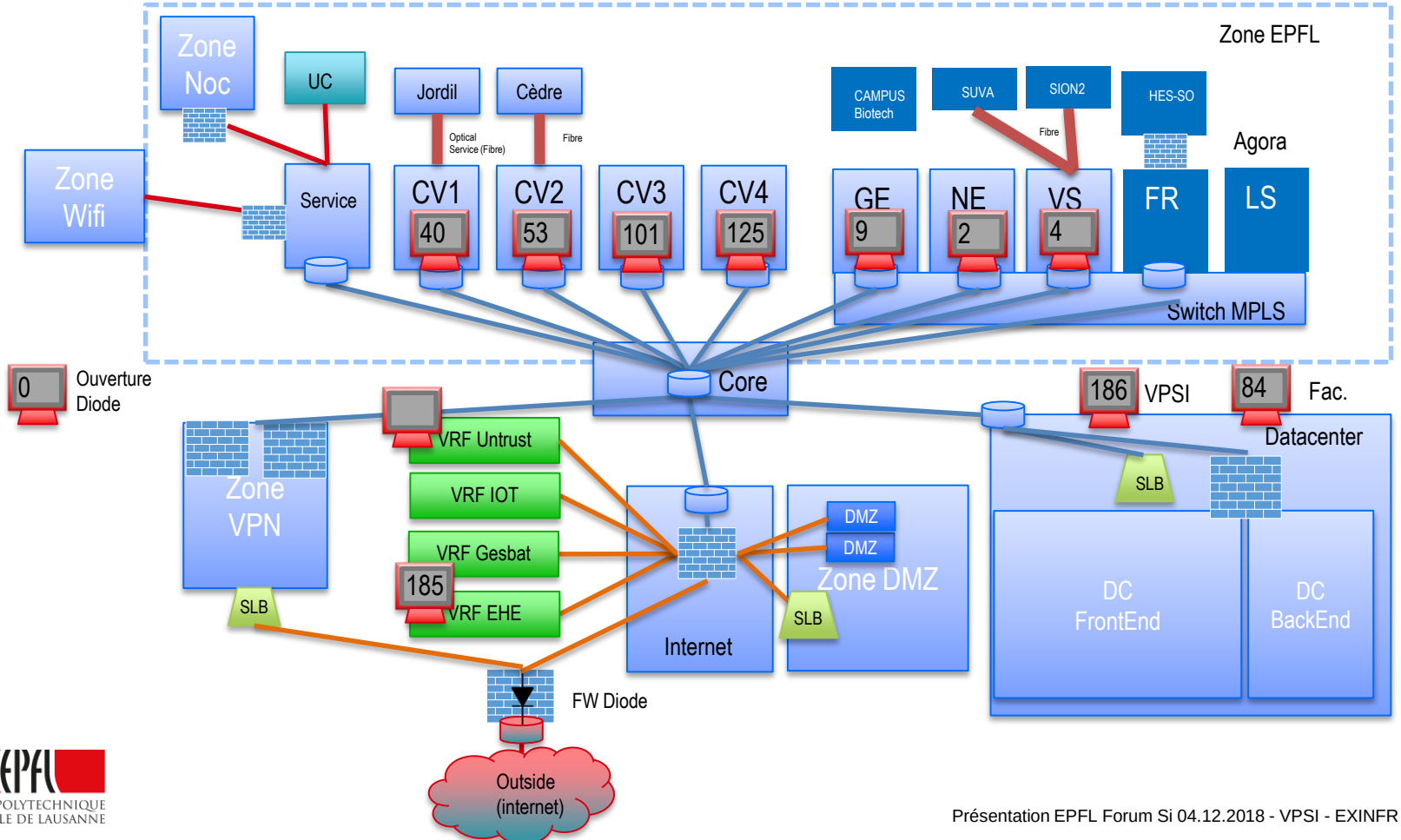
- Ouvert
- Partiellement ouvert
- Fermé
- Trafic zone à zone

Les règles de sécurités s'appliquent à des subnet composant les zones.

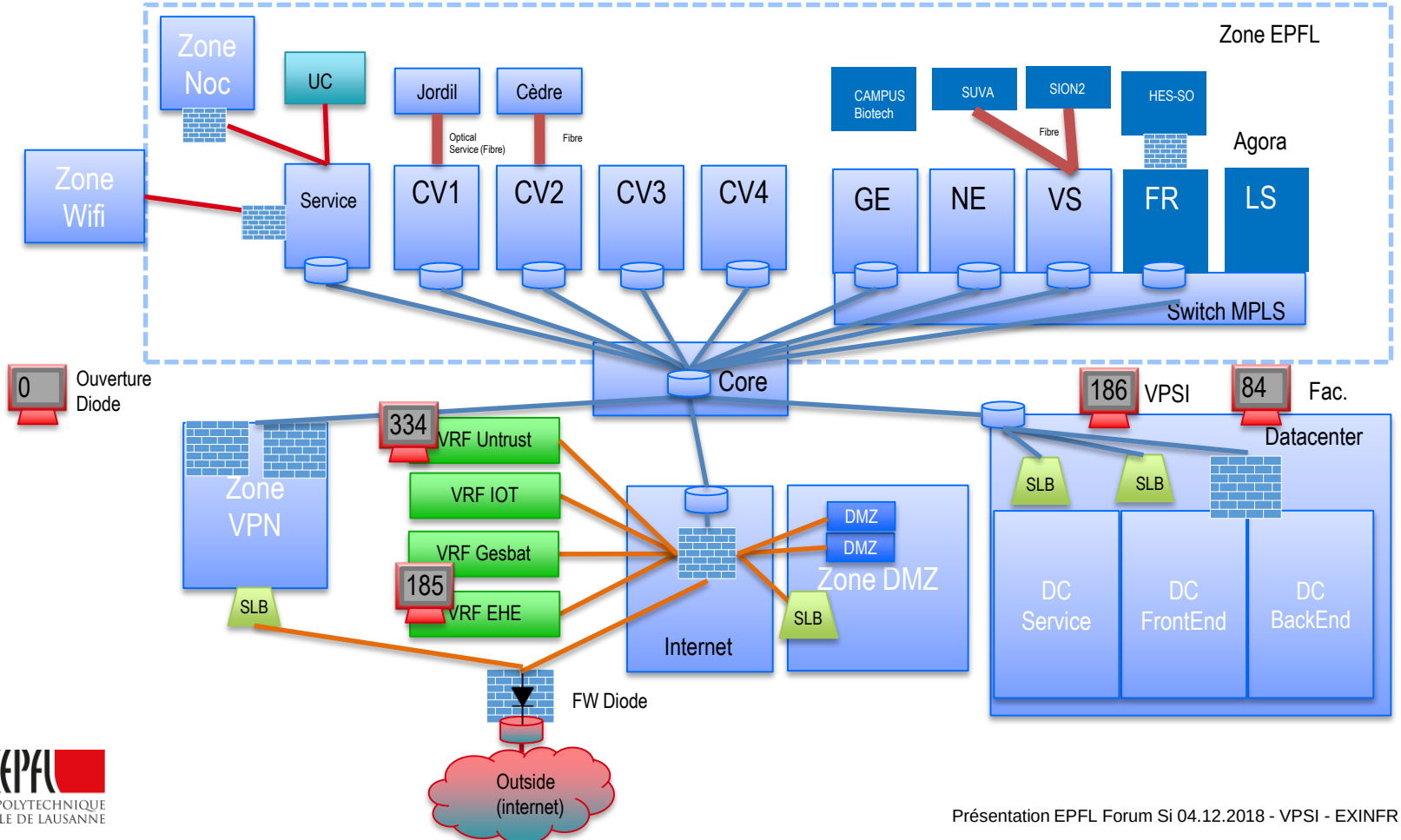
Il n'y a pas de règles spécifiques à une machine.

Phase 2

Réseau EPFL 2018 Phase1



Réseau EPFL 2018 Phase2



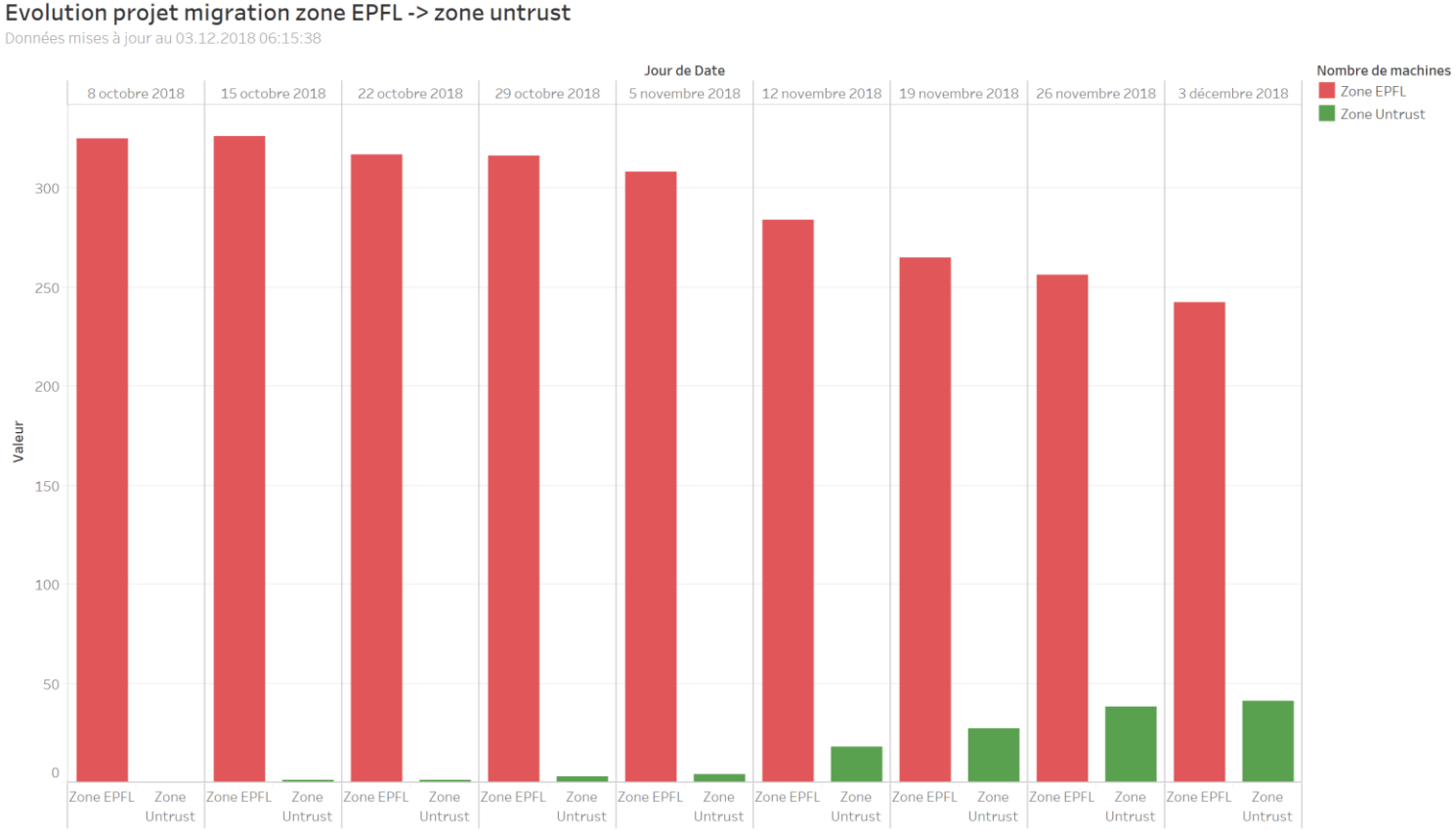
Projet phase 2

- Définir et implémenter la zone de service
    - Document de référence des services DC
    - Implémentation de la matrice pour les zones DC
    - Mise en place du monitoring des flux réseau
- Test et validation avec les clients pilotes dans les zones
- Mise à disposition de l'automate, dès le 1er octobre 2018
    - Pour le campus et à partir du 15 novembre 2018, seules les ouvertures DIODE dans la Zone Untrust seront autorisées validées par le CSI du même jour.

Projet phase 2 – Suppression des ouvertures DIODE dans EPFL

- Inventaire détaillé de toutes les ouvertures DIODE
- Macro planning de la migration avec suivi de l'avancement
- Phase de migration des 334 machines se déroule entre le 1 octobre 2018 et 31 mars 2019
    1. EXINFR prend contact avec le responsable des machines
    2. Identification des besoins
    3. Planification de la migration avec le responsable des machines
    4. Préparation de la migration avec monitoring des flux
    5. Migration et validation du fonctionnement

Histogramme



Projet phase 3

- Documentation
  - Révision finale de la politique de sécurité
  - Mise à jour des documents du projet
- Audit et finalisation du projet
  - Mandater une société externe
  - Remise des documents
  - Validation finale et fermeture du point d'audit du CEPF

Rappels !

Vous pouvez trouver toutes les informations liées à ce projet sur les liens suivants :

https://epnet.epfl.ch
https://support.epfl.ch/epfl?id=kb_article_view&sysparm_article=KB0014360
https://network.epfl.ch/xtrn/download/directives/VRF-Segmentation-2018.pdf
https://network.epfl.ch/xtrn/download/directives/Aide_migration_DIODE_Untrust.pdf
https://network.epfl.ch/xtrn/download/directives/EPFL_Directives_EPNET.pdf

Question/Discussion

Merci pour votre attention.