Sécurité réseau pour applications en conteneur

Martin Ouimet
Solution Architect,
Cloud Specialist

Red Hat

Agenda

- Kubernetes et SDN
- Questions relatives à la sécurité des réseaux en entreprise
  - Restriction du trafic entre les différents “Tiers”
  - Micro-segmentation
  - Sécuriser le trafic sortant
  - Sécuriser le trafic entrant
- Securité des applications avec Service Mesh

Kubernetes est clairement le gagnant de l'orchestration des conteneurs à travers le monde.

Que manque-t-il pour rendre Kubernetes prêt pour les entreprises ?

Kubernetes

Red Hat

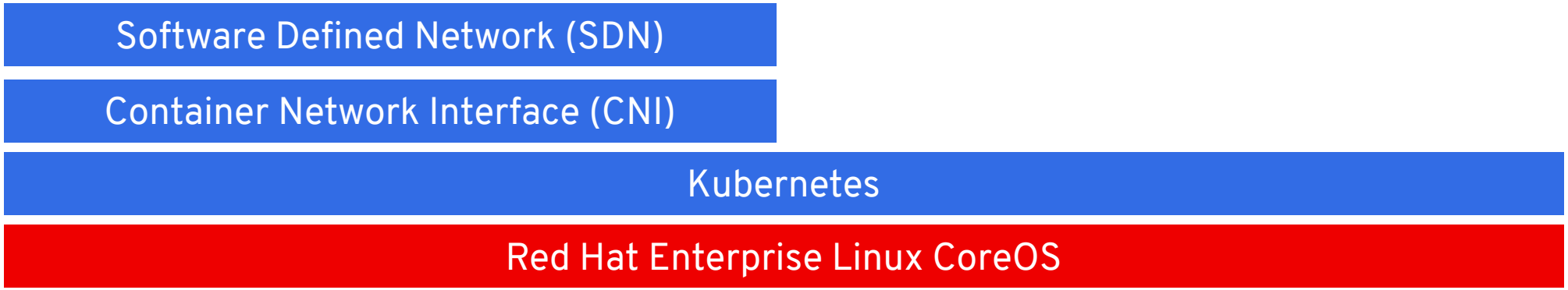
Un système d'exploitation **sécuritaire**, conçu pour les **entreprises** et **optimisé** pour les conteneurs

Kubernetes

Red Hat Enterprise Linux CoreOS

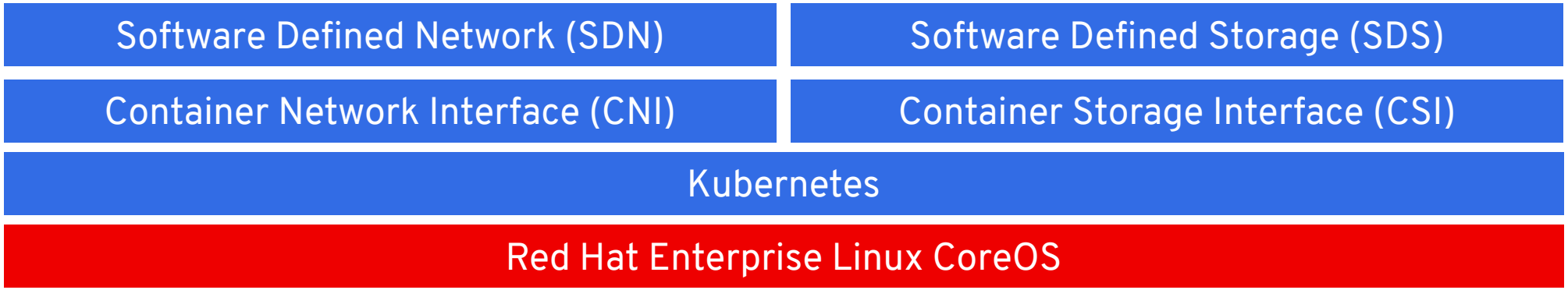
Red Hat

Interface moderne et **flexible** de gestion du **réseau**



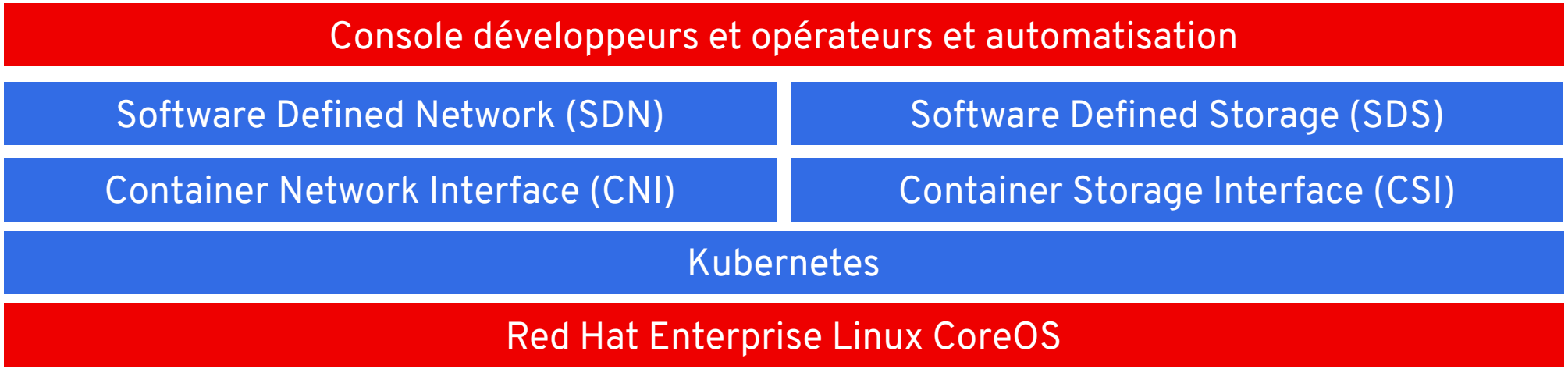
Red Hat

Interface moderne et **flexible** de gestion du **stockage**



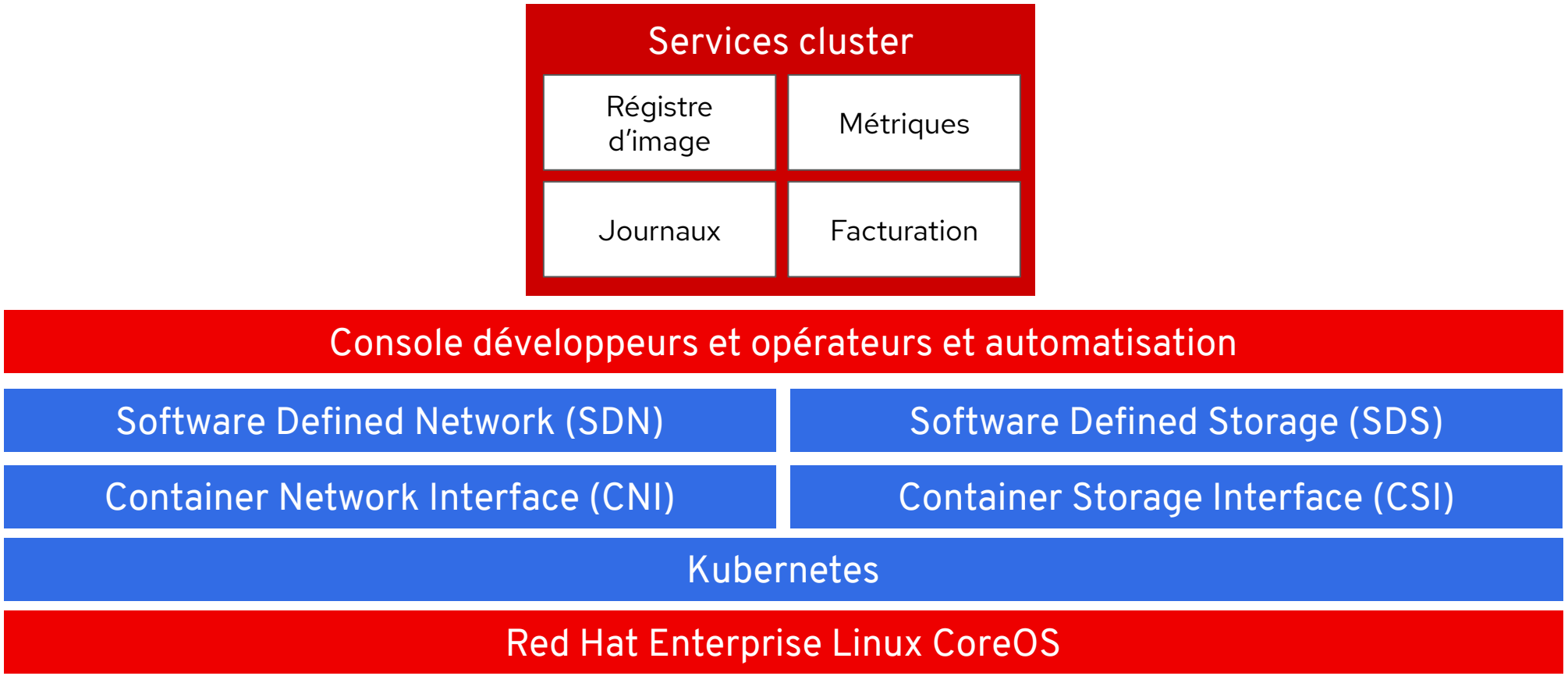
Red Hat

Outils de gestion du cluster et du cycle de vie des composantes logiciels.



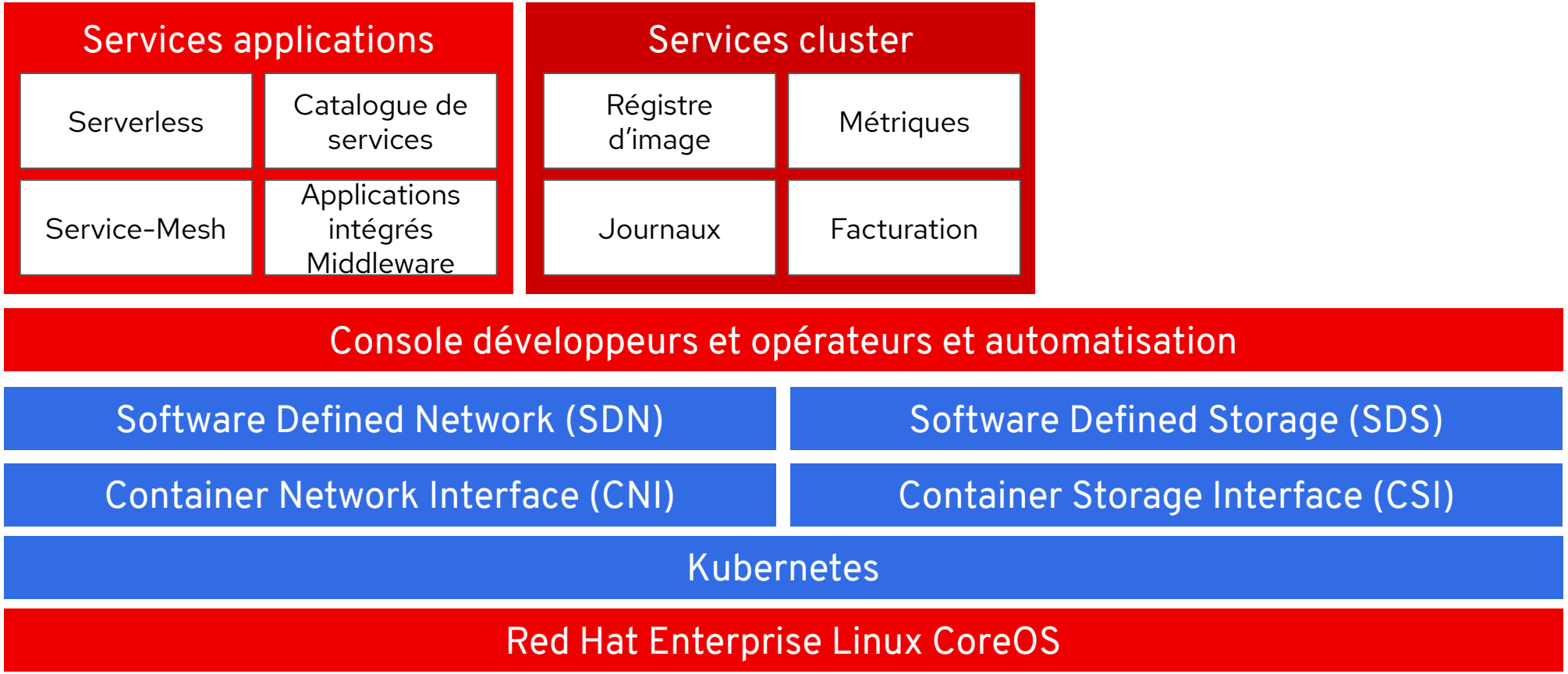
Red Hat

Registre de conteneurs sécurisé, journaux, métriques, outils de facturation (chargeback)



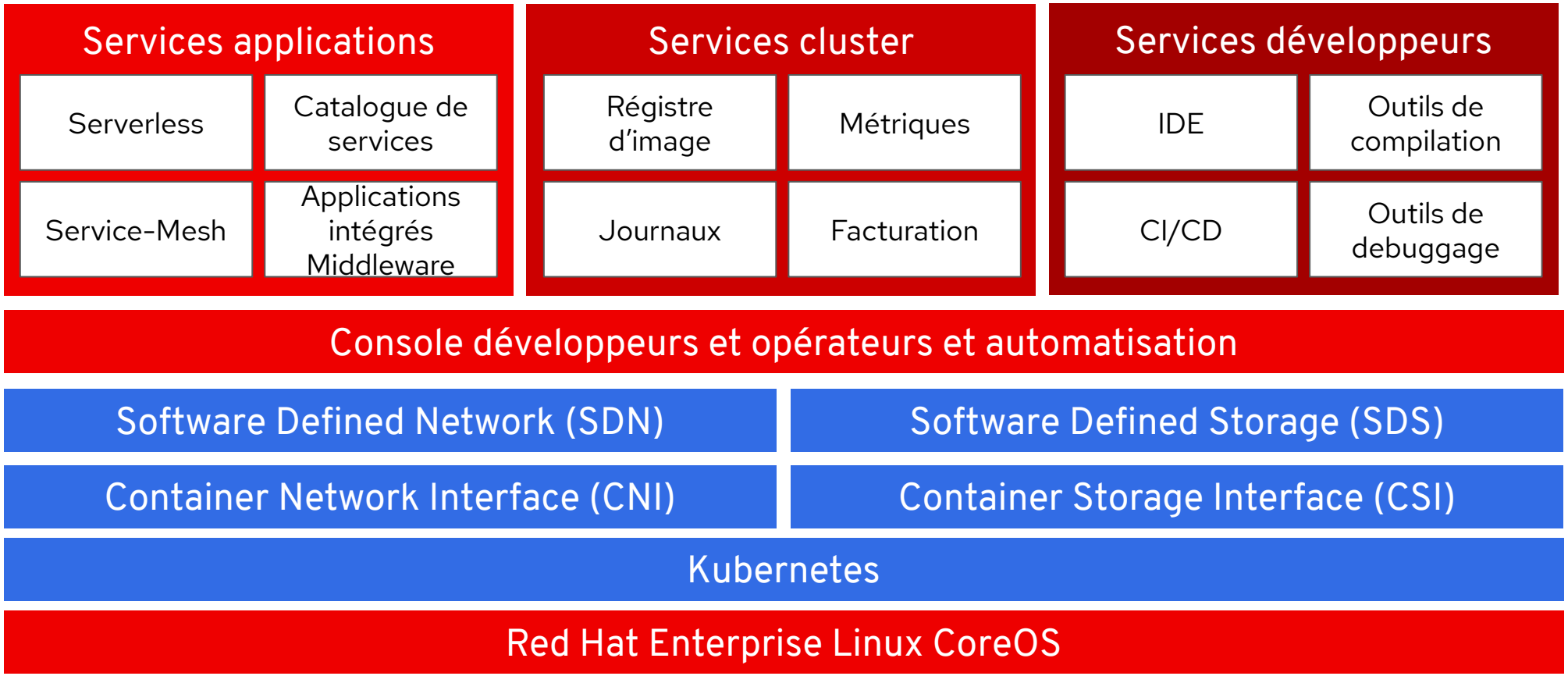
Red Hat

Standardiser la couche logicielle “Middleware”, avoir un catalogue de service et des outils de gestion pour micro-services

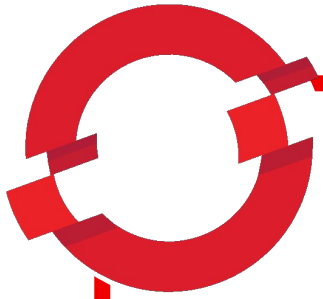


Red Hat

Développeurs ont besoin de IDE, gestionnaire de compilation, CI/CD, utilitaires de debuggage et plus encore !



Red Hat



Plateforme d'orchestration de conteneurs pour entreprises

Services applications		Services cluster		Services développeurs	
Serverless	Catalogue de services	Régistre d'image	Métriques	IDE	Outils de compilation
Service-Mesh	Applications intégrés Middleware	Journaux	Facturation	CI/CD	Outils de debuggage

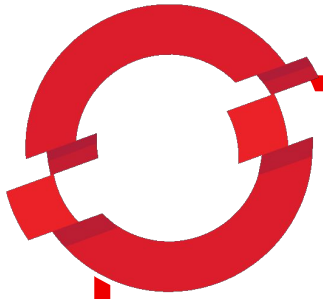
Console développeurs et opérateurs et automatisation

Software Defined Network (SDN) | Software Defined Storage (SDS)

Container Network Interface (CNI) | Container Storage Interface (CSI)

Kubernetes

Red Hat Enterprise Linux CoreOS



Plateforme d'orchestration de conteneurs pour entreprises

Services applications		Services cluster		Services développeurs	
Serverless	Catalogue de services	Régistre d'image	Métriques	IDE	Outils de compilation
Service-Mesh	Applications intégrés Middleware	Journaux	Facturation	CI/CD	Outils de debuggage

Console développeurs et opérateurs et automatisation

Software Defined Network (SDN)	Software Defined Storage (SDS)
Container Network Interface (CNI)	Container Storage Interface (CSI)

Kubernetes

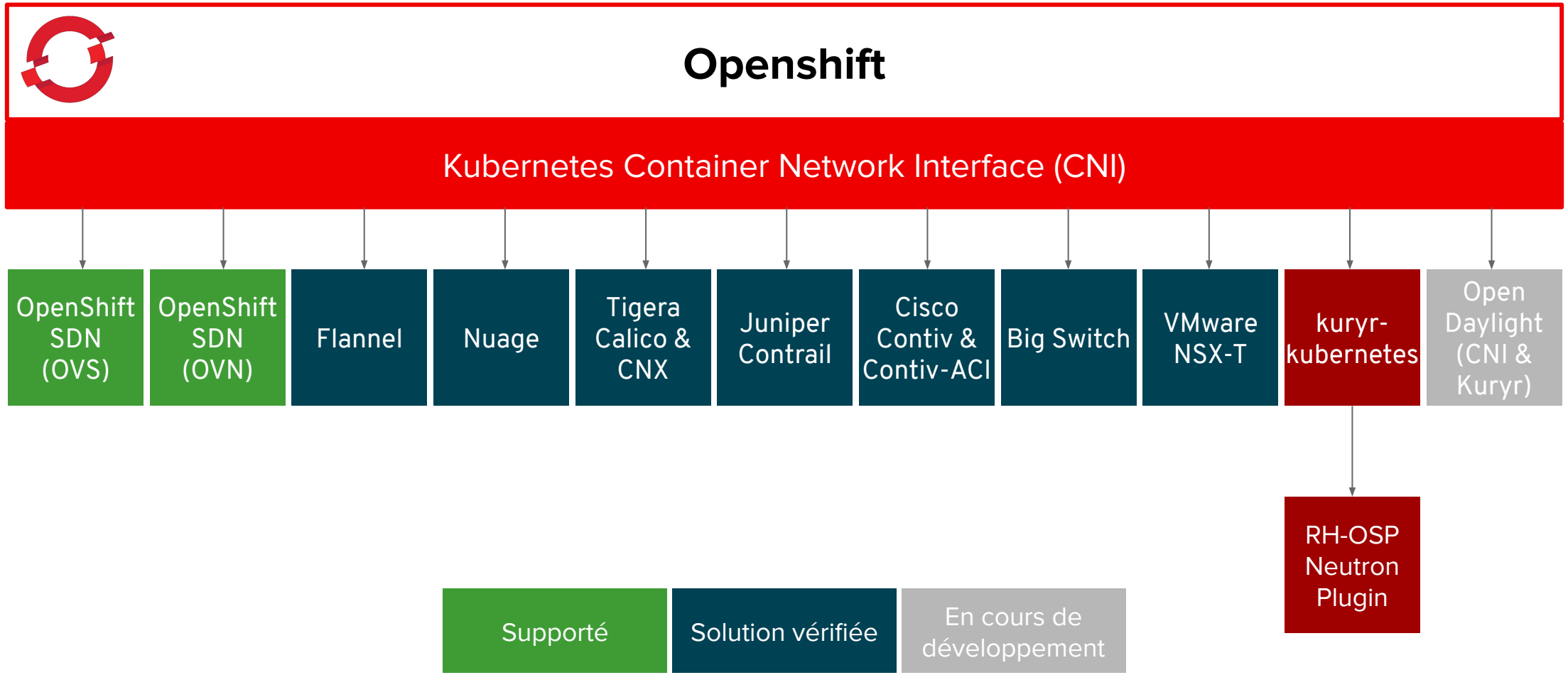
Red Hat Enterprise Linux CoreOS

Qu'est-ce que Software Defined Network ?

Et pourquoi est-ce important ?

Red Hat

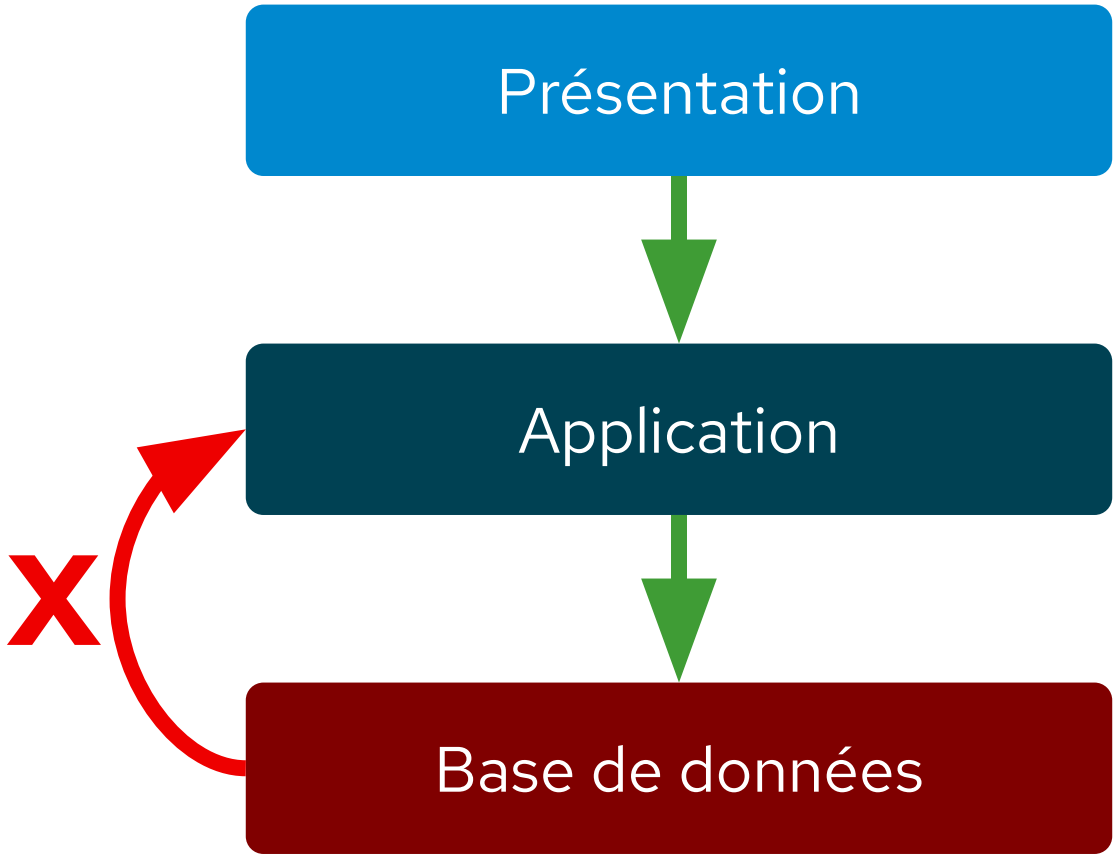
Connecteurs réseau pour Openshift



Red Hat

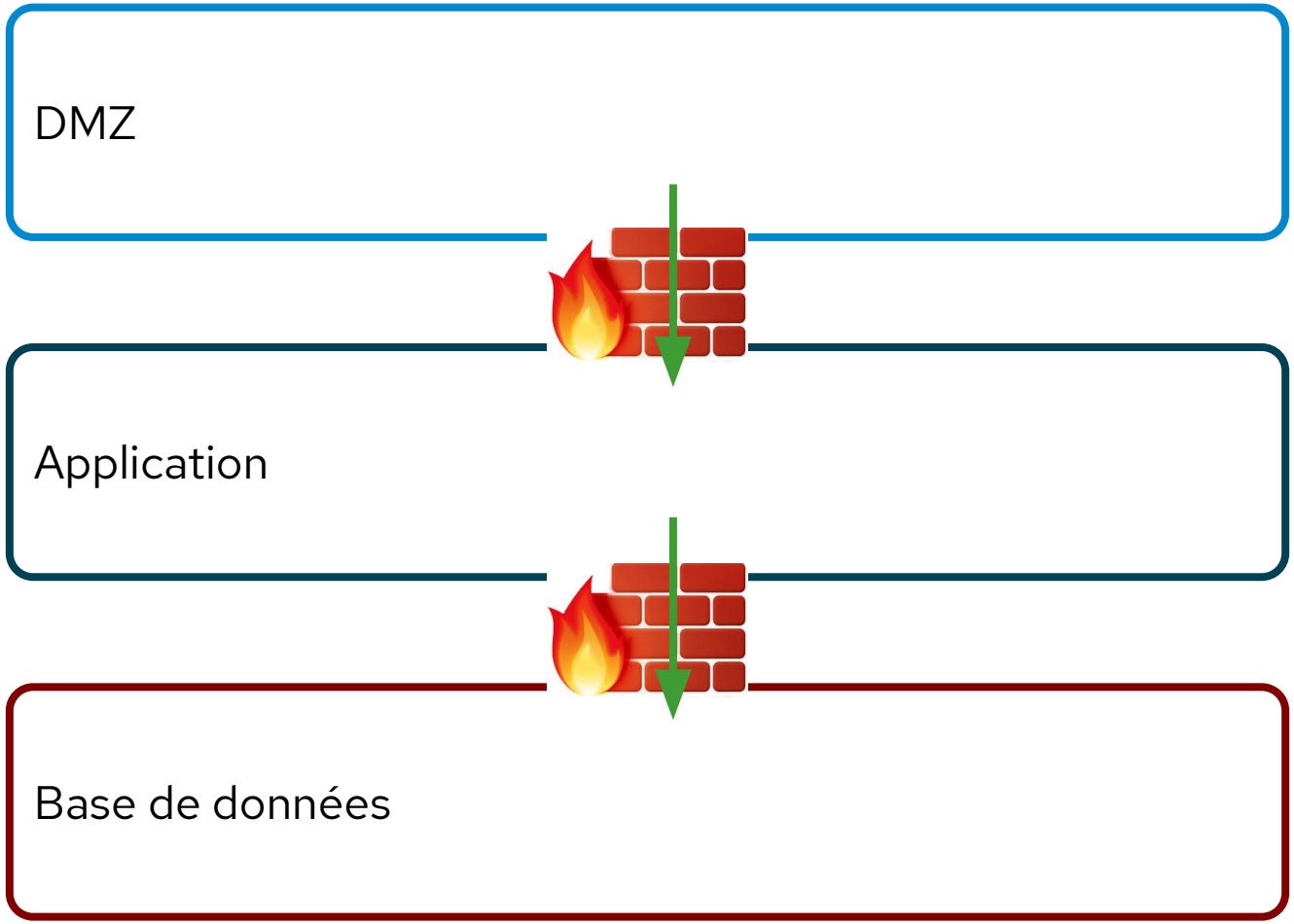
Isoler les zones

Restreindre le trafic entre les “tiers”



Red Hat

Les coupe-feux externes sont requis entre les zones



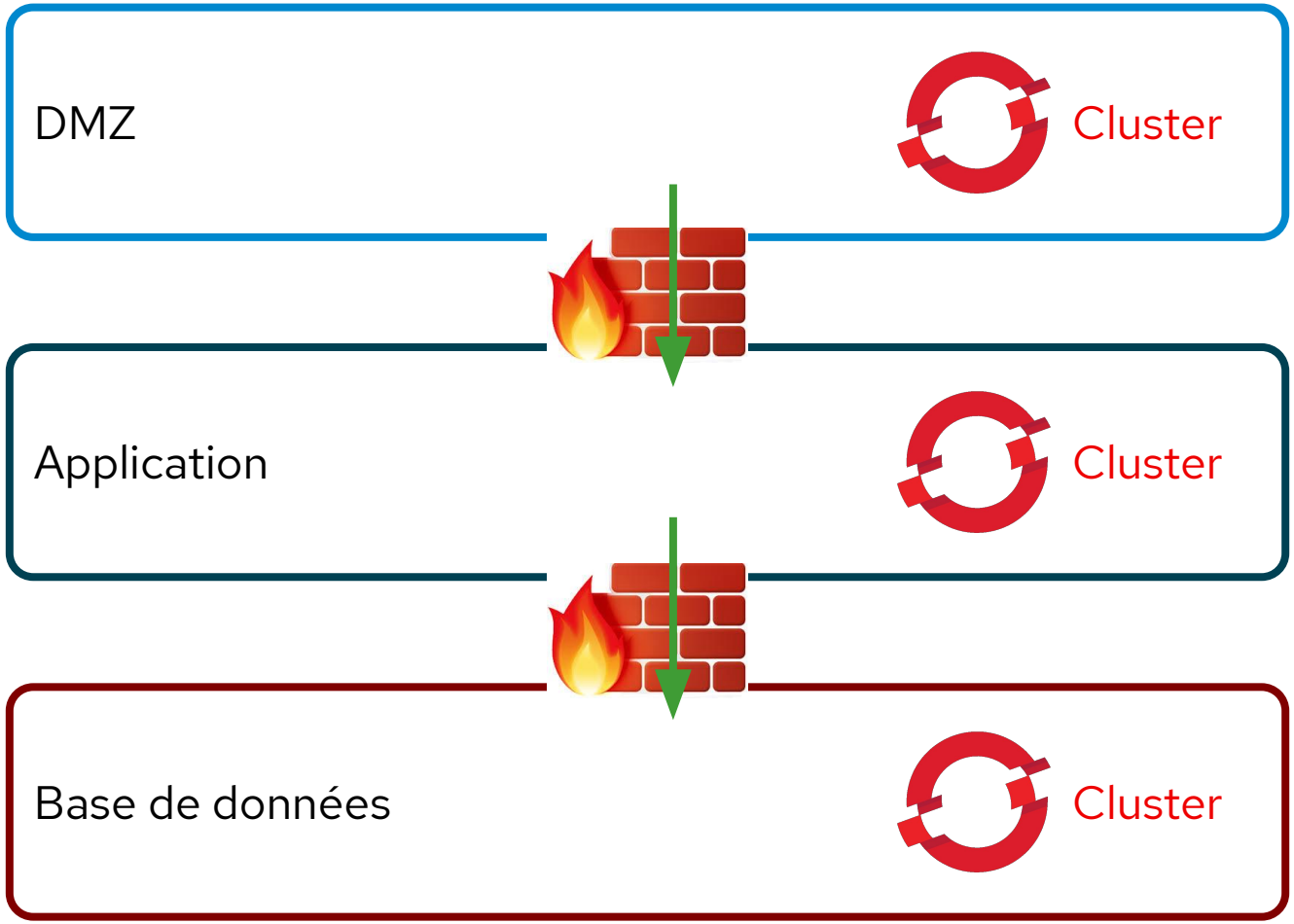
Le trafic provenant de Internet est permis vers la zone délimitarizée.

Ouverture coupe-feu pour permettre les flows suivants:

- Zone DMZ vers la zone applicative
- Zone applicative vers la zone de base de données.

Comment accomplir un montage similaire avec Kubernetes ?

Les coupe-feux externes sont requis entre les zones

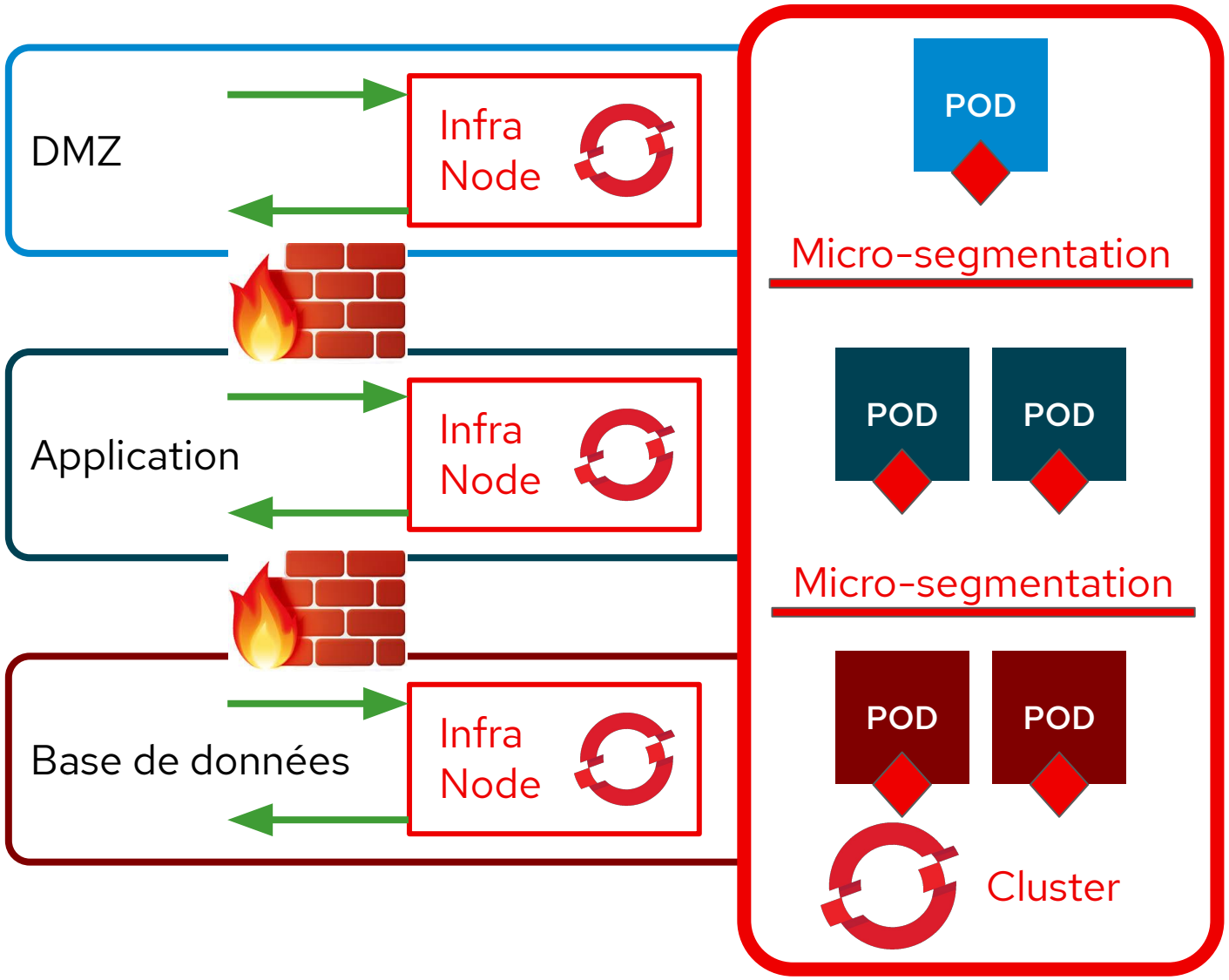


Montage aligné avec les standards de sécurité établis

Le coupe-feu ne prévient pas nécessairement l'accès aux outils de gestion du Cluster et demande des configurations additionnelles.

Coûts d'opérations et de maintenance d'une telle infrastructure sont élevés.

Les coupe-feux externes sont requis entre les zones



Un seul cluster à gérer

Utilisation des Network Policy Object pour effectuer la micro-segmentation

Les Infra Nodes exécutent les fonctions de Ingress et Egress spécifiques à chaque zone.

Red Hat

Network Policy Objects

Gestion de la micro-segmentation

Configurer des politiques individuelles au niveau des PODs

Restreint le trafic entre les PODs à l'intérieur du projet

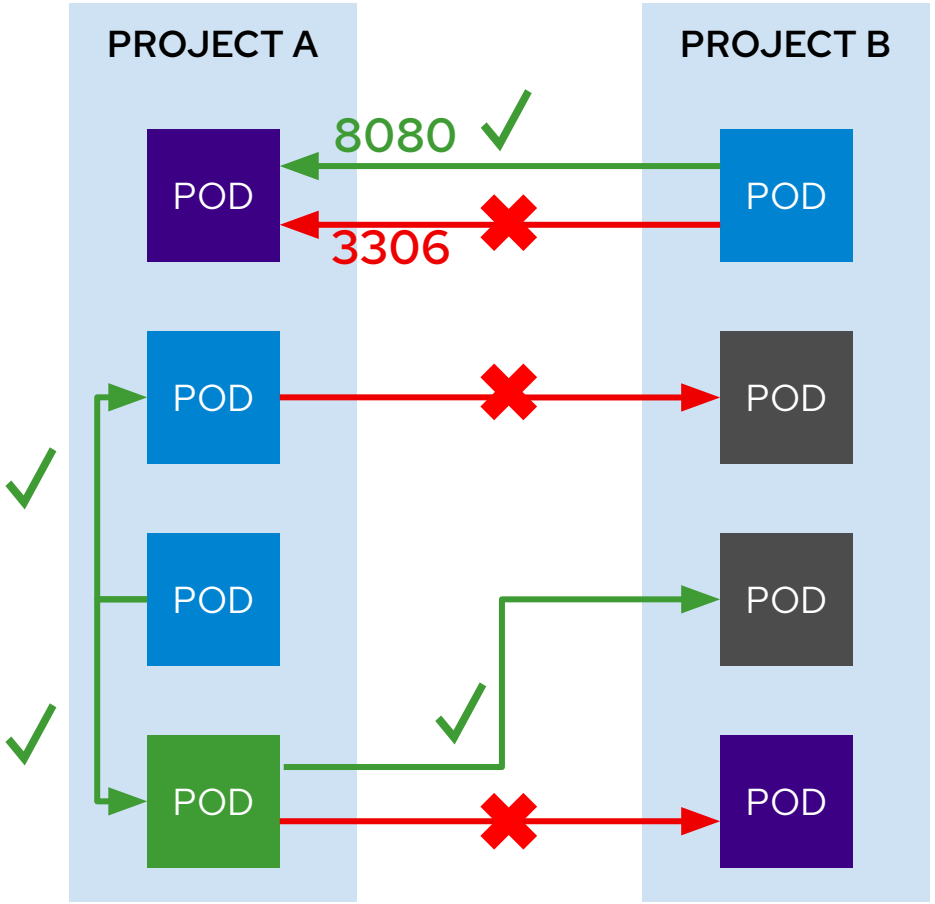
Appliquées sur trafic entrant des services et des PODs

Permet le trafic d'un autre projet vers un POD spécifique

Et la micro-segmentation…

est-ce mieux que la sécurité traditionnelle telle qu'on la connaît depuis des années ?

Network Policy Objects

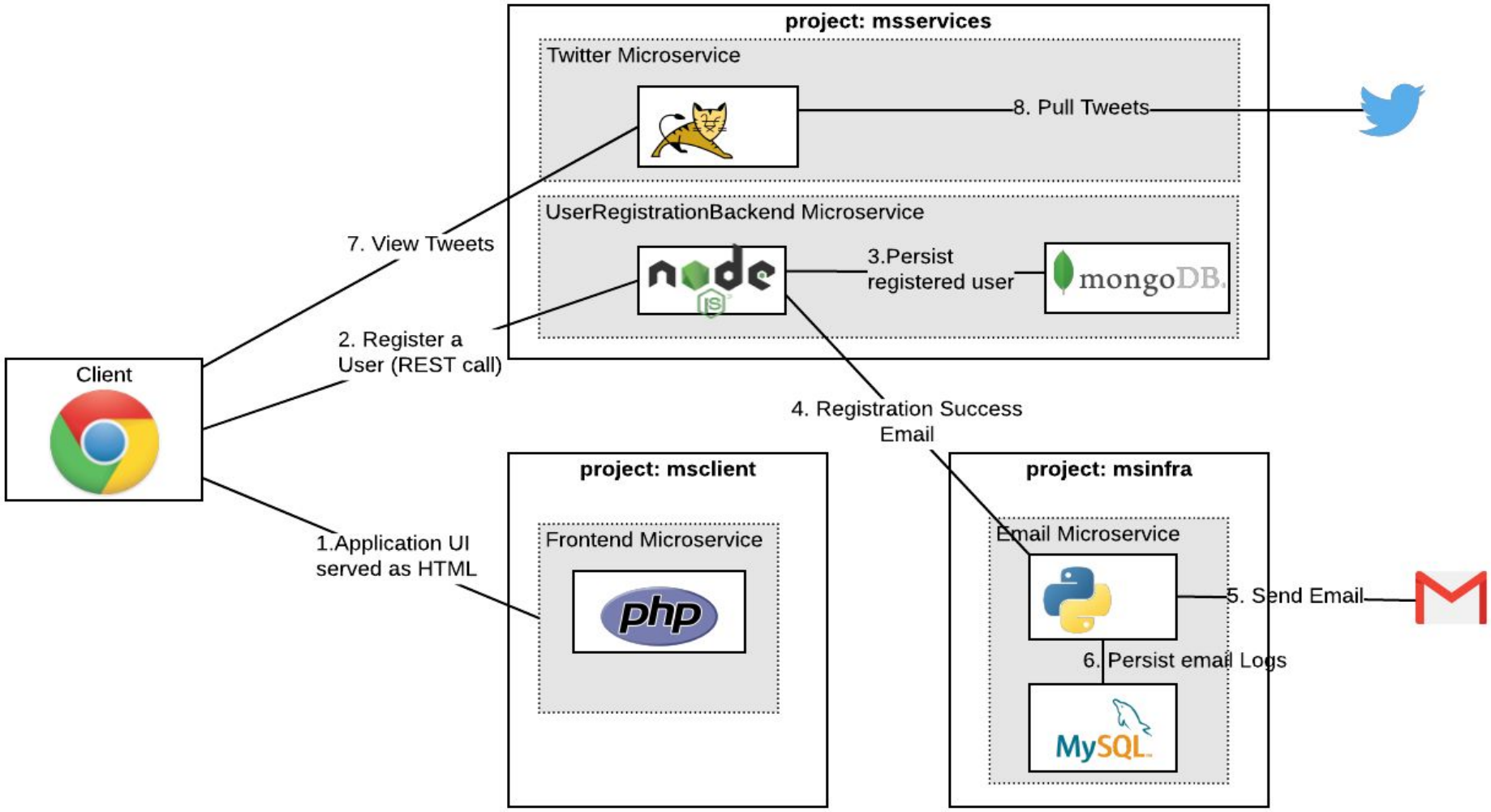


Examples de Policy Objects

- Permettre tout le trafic à l'intérieur du projet
- Permettre le trafic de Vert vers Gris
- Permettre le trafic vers Violet sur le port 8080

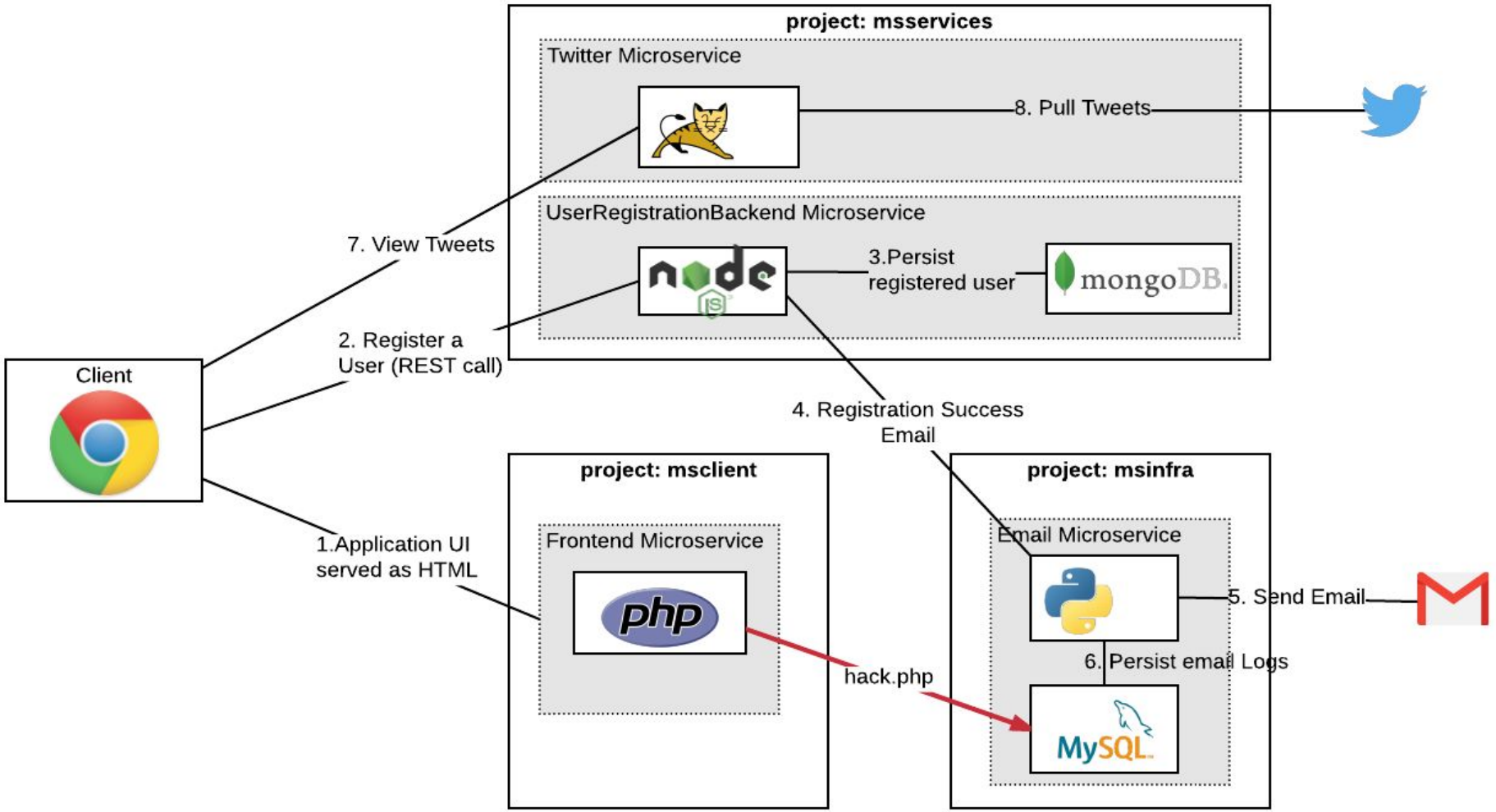
```
apiVersion: extensions/v1beta1
kind: NetworkPolicy
metadata:
  name: allow-to-purple-on-8080
spec:
  podSelector:
    matchLabels:
      color: purple
  ingress:
  - ports:
    - protocol: tcp
      port: 8080
```

Exemple: Application web typique avec séparation du frontal et api



Red Hat

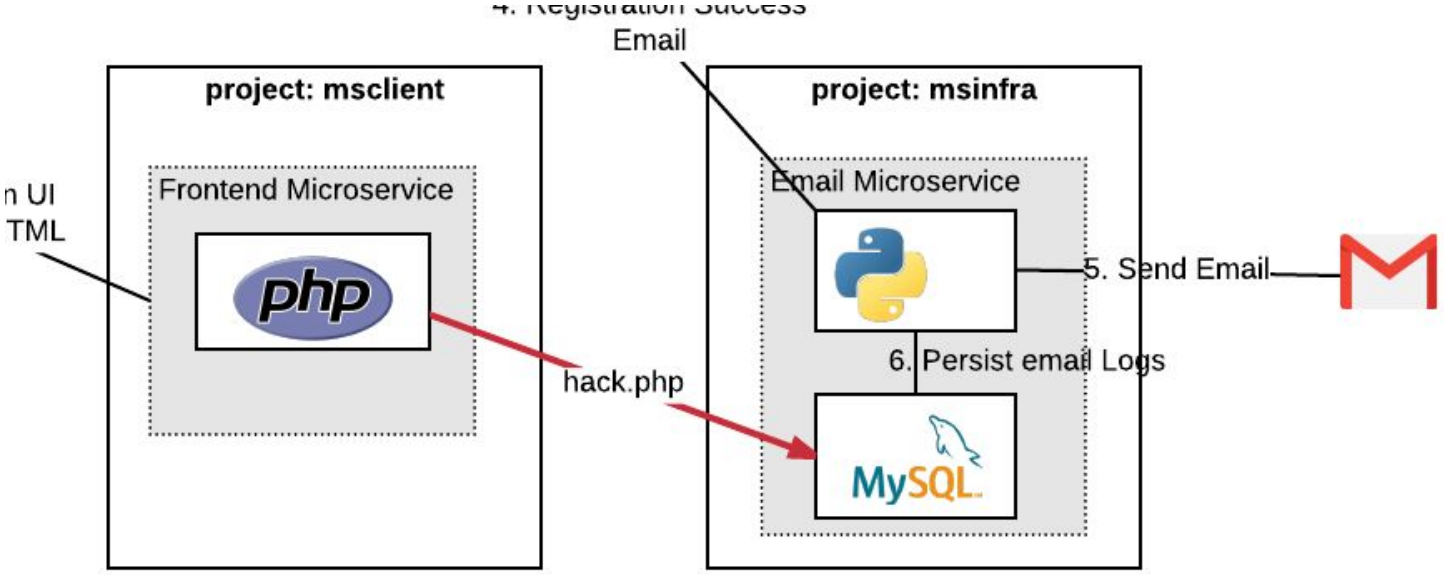
Exemple: Un fichier malicieux est exécuté sur le serveur PHP



Red Hat

Les Network Policy Objects a la rescousse !

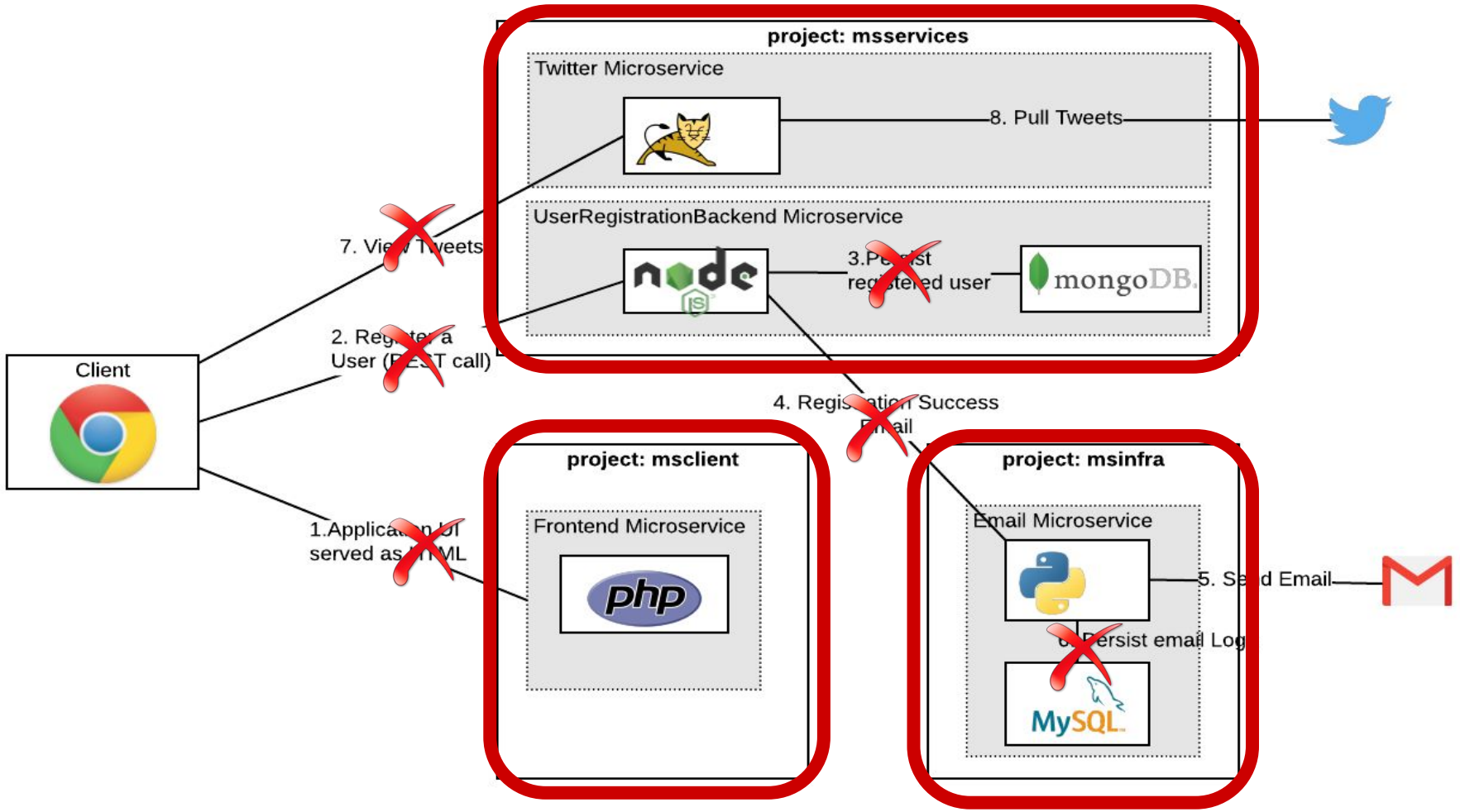
Permettre la connexion à MySQL uniquement depuis le service email.




```
kind: NetworkPolicy
apiVersion: extensions/v1beta1
metadata:
  name: allow-3306
spec:
 podSelector:
   matchLabels:
     app: mysql
 ingress:
 - from:
   - podSelector:
       matchLabels:
         app: emailsvc
   ports:
   - protocol: TCP
     port: 3306
```

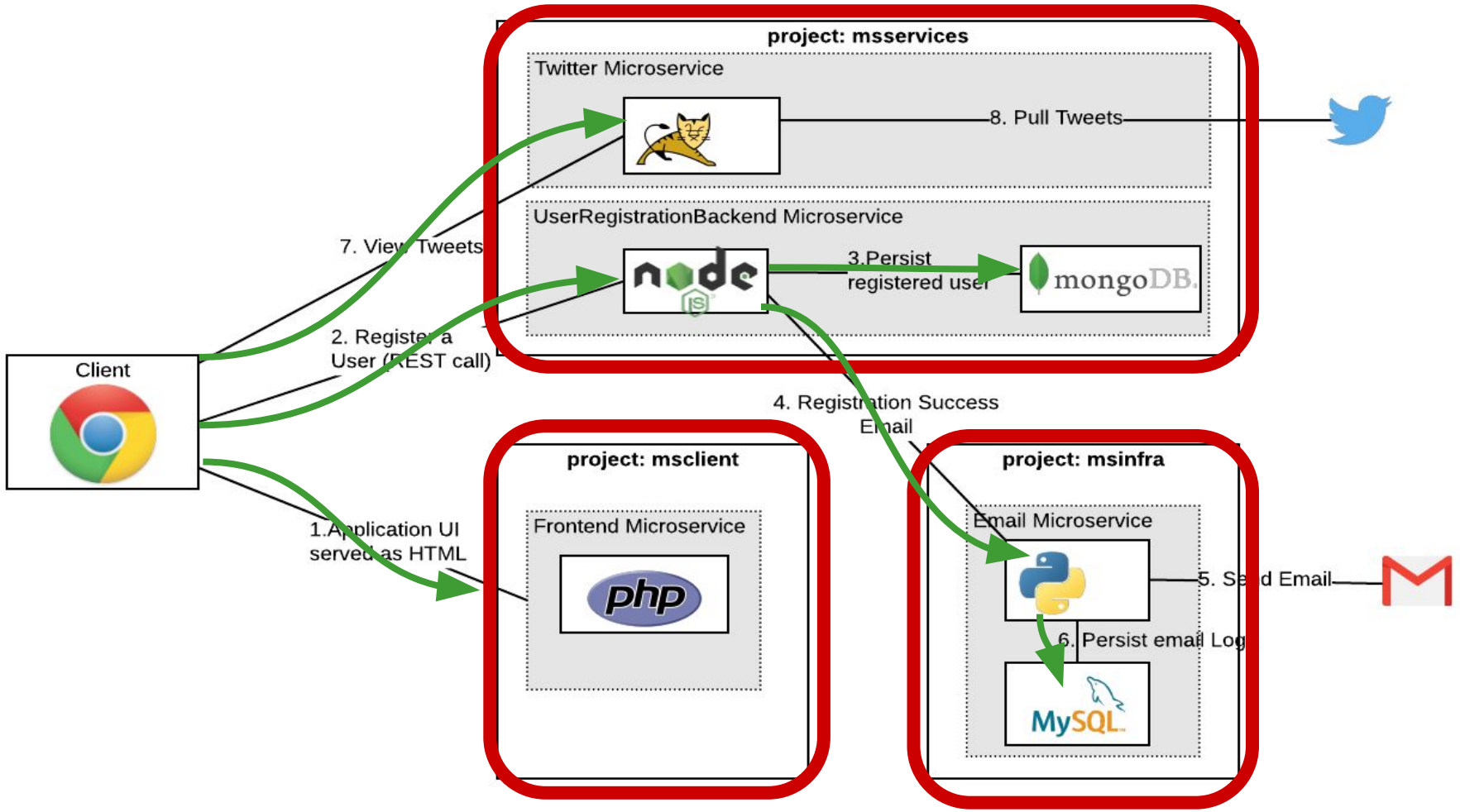

Red Hat

Commencez avec un “Deny” par défaut



Red Hat

Utilisez les Network Policy pour permettre les flows spécifiques



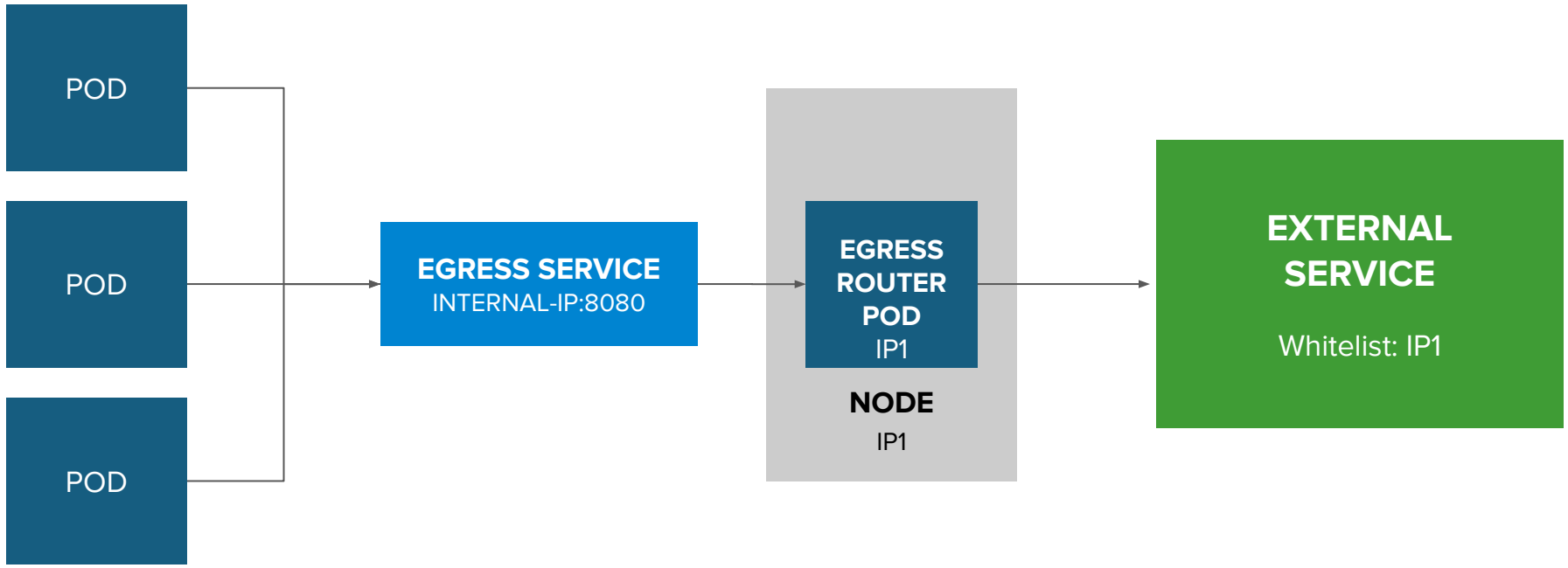
Red Hat

Sécuriser le trafic en sortie

Egress

Contrôler le trafic sortant avec le Egress Router

Contrôler la DESTINATION IP

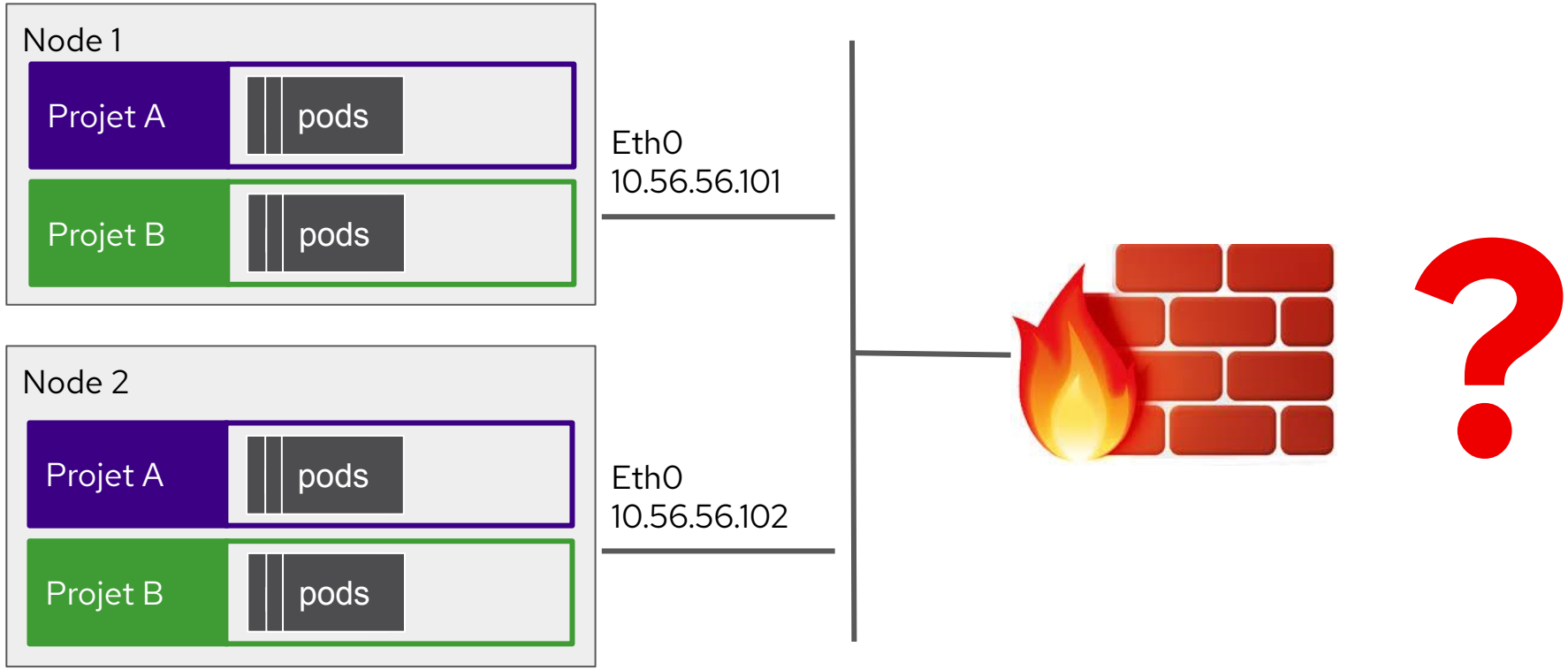


Red Hat

Controller le trafic sortant (Egress)

Contrôler la SOURCE IP

Comment reconnaître le trafic de sortie du cluster Openshift ?

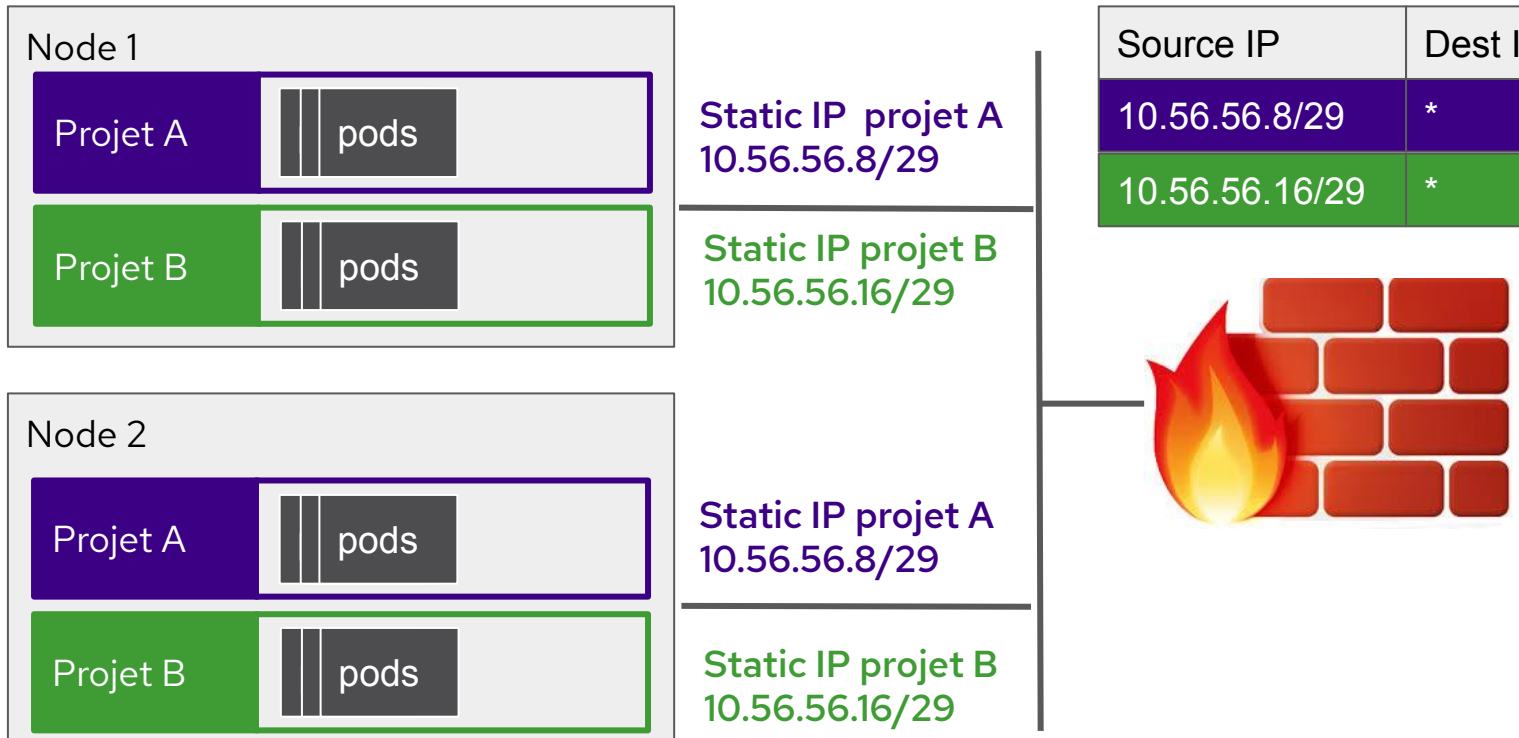


Red Hat

Controller le trafic sortant (Egress)

Contrôler la SOURCE IP

Comment reconnaître le trafic de sortie du cluster Openshift ?



Source IP	Dest IP	Port	Action
10.56.56.8/29	*	443	Allow
10.56.56.16/29	*	443	Deny

Red Hat

Sécuriser le trafic en entré

Ingress

Configurer ce qui doit être exposé

La sécurité commence par exposer uniquement ce qui doit être accessible depuis l'extérieur du cluster.

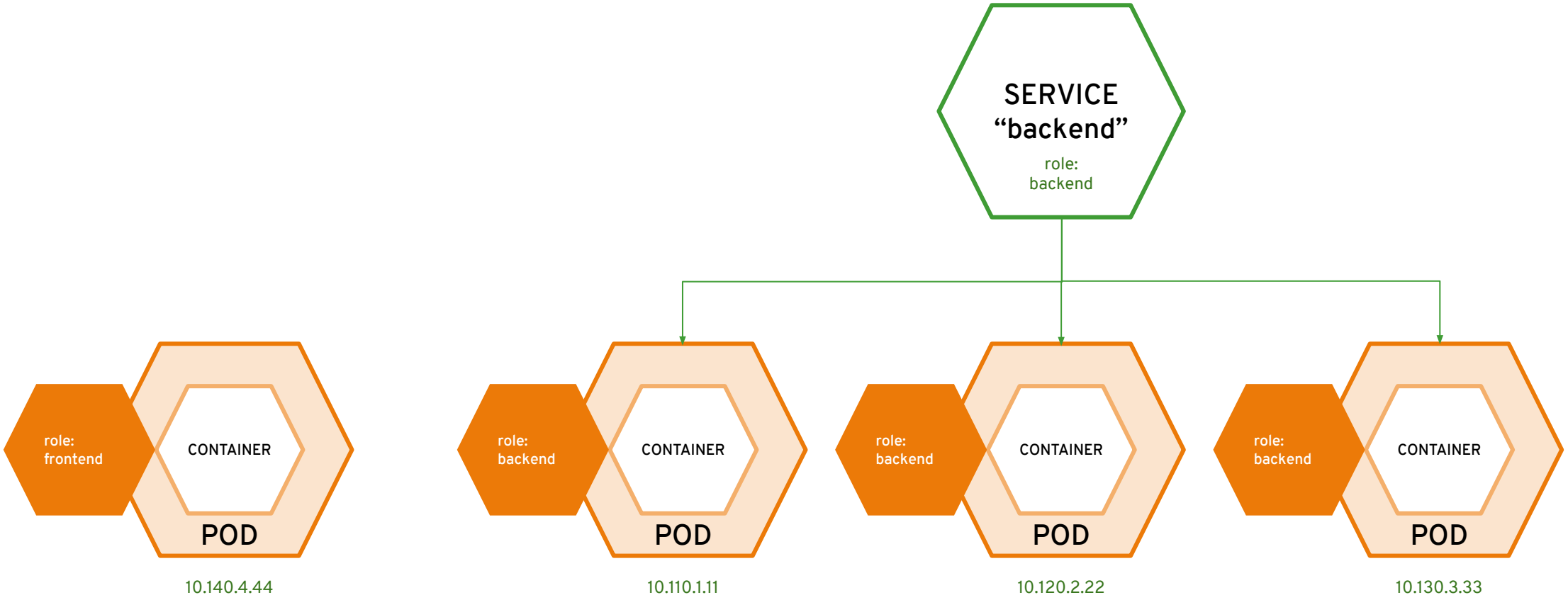
Service

Un service est un balanceur de charge qui crée un point d'entrée vers un ou plusieurs PODs. Le service peut être exposé à l'externe du cluster ou non.

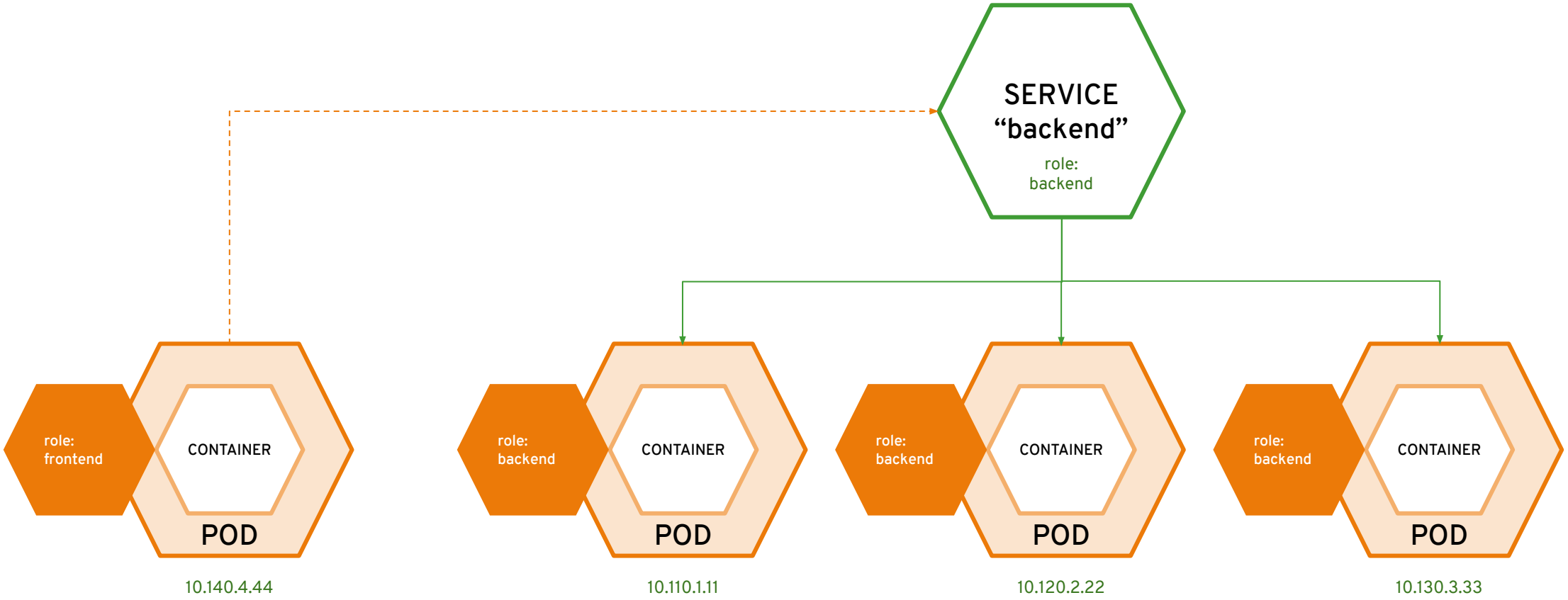
Route

Une route est un point d'entré publique HTTP ou HTTPS vers un service.

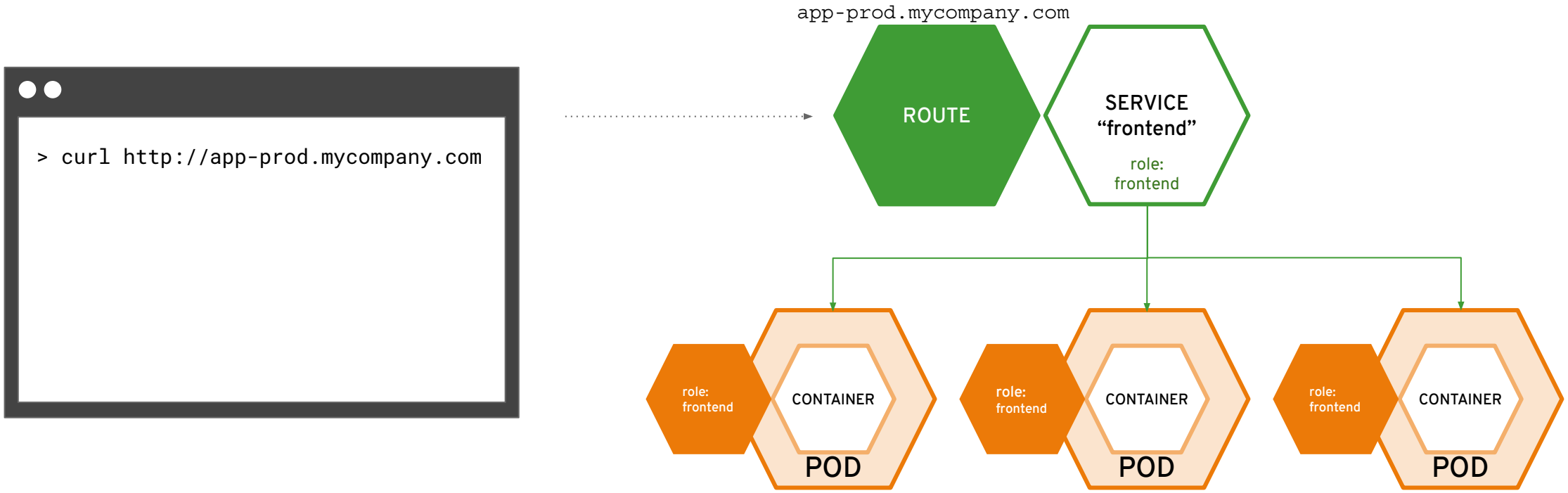
Le Service est un balanceur de charge interne qui découvre automatiquement les pods



Les applications peuvent communiquer entre eux via les services



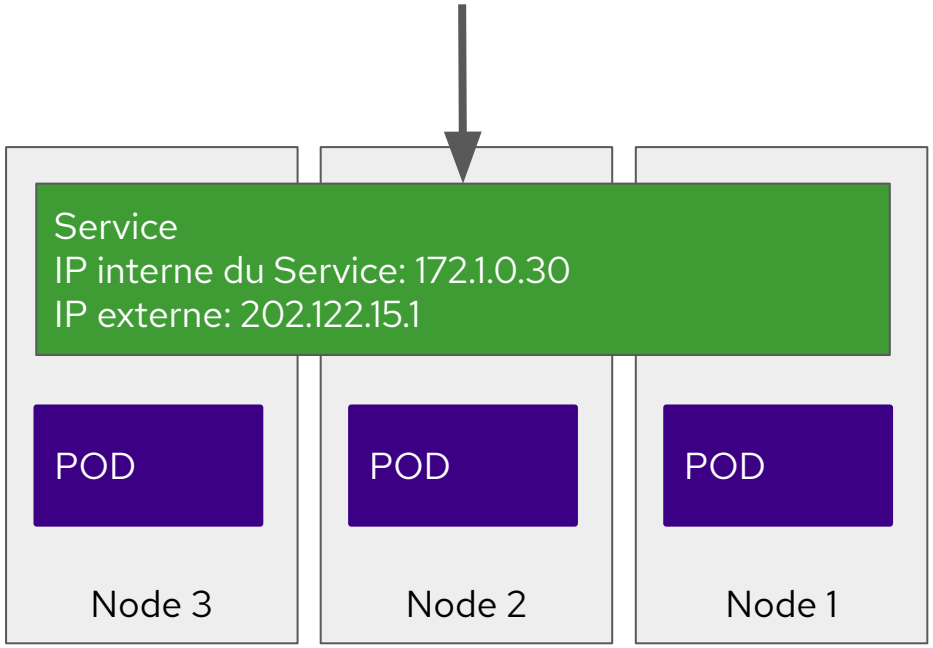
Les **routes** rendent les services accessibles au clients à l'extérieur de l'environnement en utilisant des **URLs**



Red Hat

Contrôler le trafic en entrée (Ingress)

Un service peut être exposé directement sur un port TCP.



L'administrateur du cluster définit une plage d'adresses IP qui peuvent être assignées à des noeuds ou des services.

Opensihft assigne l'adresse IP privée et publique au service.

Le noeud sur lequel l'adresse IP est assignée agit de point d'entré pour le service.

L'adresse IP externe peut être une VIP. En configurant ip-failover, la VIP peut être réassignée à d'autre noeuds.

Sécuriser les routes avec un “whitelist”

- L’accès à la route est restreinte aux adresses IP définies par le whitelist
- Configuration simple via annotations
- La connexion à la route par d’autres adresses IP sont bloqués

```
metadata:
  annotations:
    haproxy.router.openshift.io/ip_whitelist: 192.168.1.10 192.168.1.11
```

Encryption SSL sur les routes HTTP

Terminaison SSL au niveau de la route
(Certificat sur la route uniquement)

SSL Passthrough
(Certificat géré par l'application)

Réencryption
(Certificat sur la route + dans l'application)

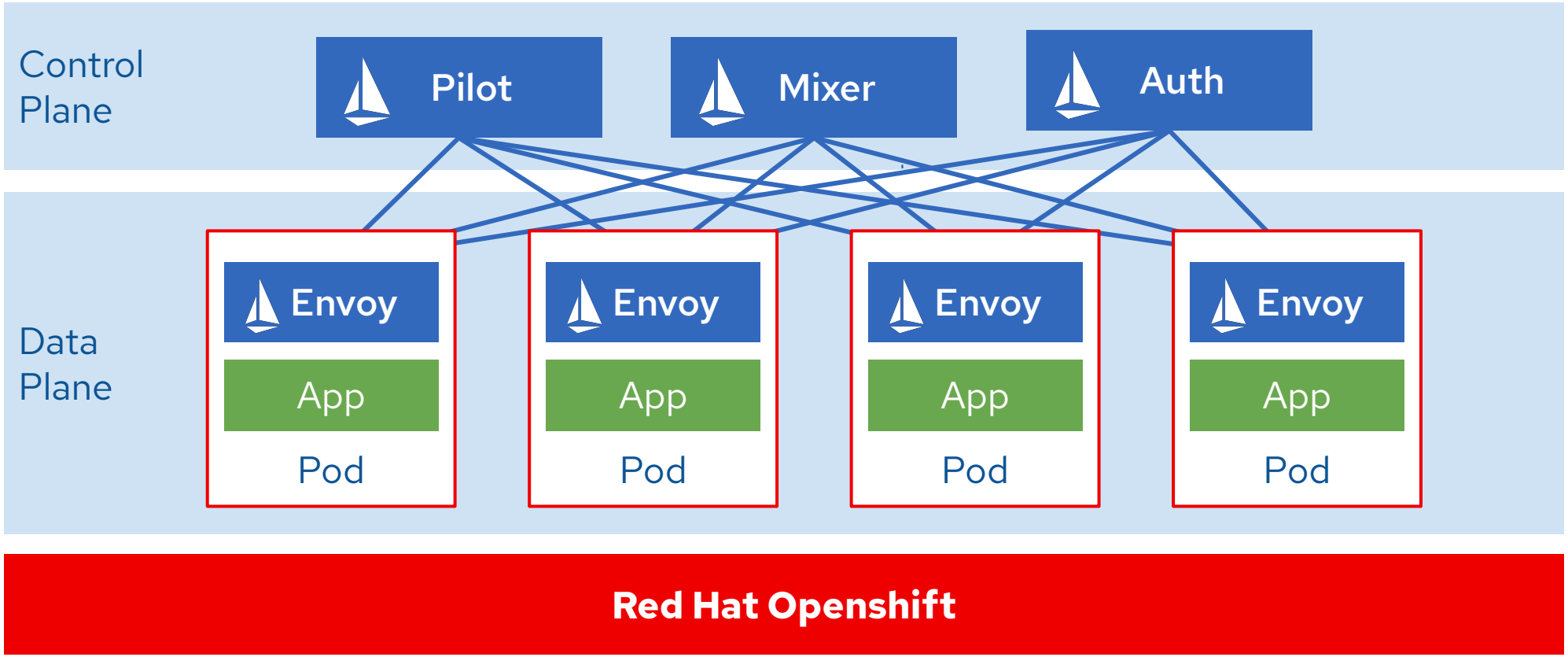
Red Hat

Sécuriser au niveau de l'application

Service Mesh

Qu'est ce que Istio ?

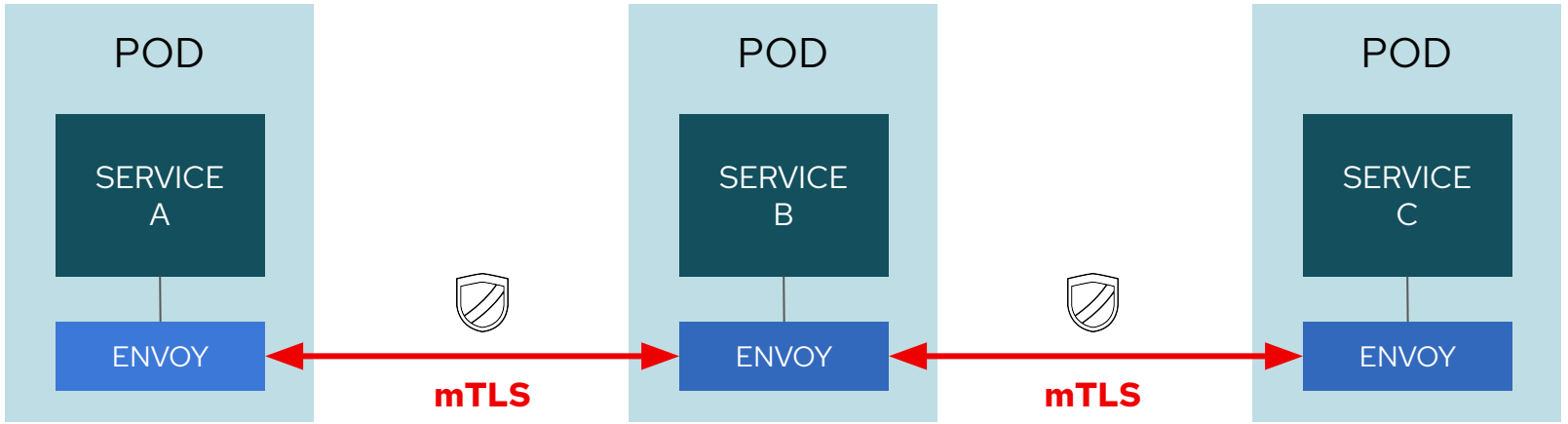
Service Mesh



Red Hat

Sécuriser les applications avec Service Mesh

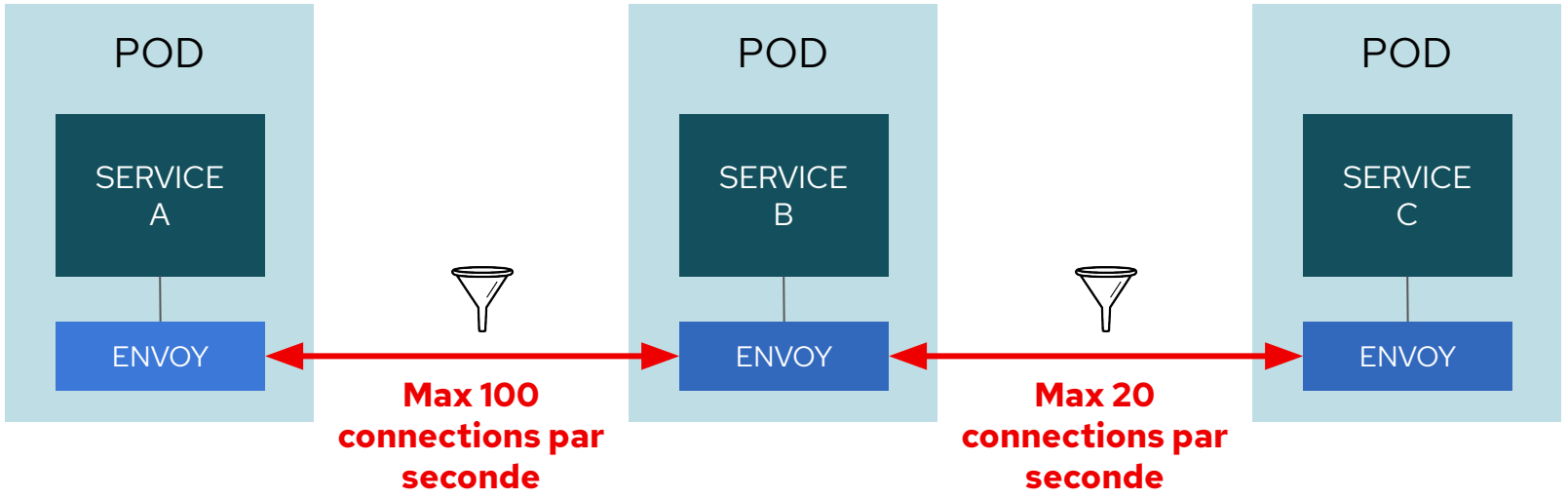
Authentification mutuelle TLS



Red Hat

Sécuriser les applications avec Service Mesh

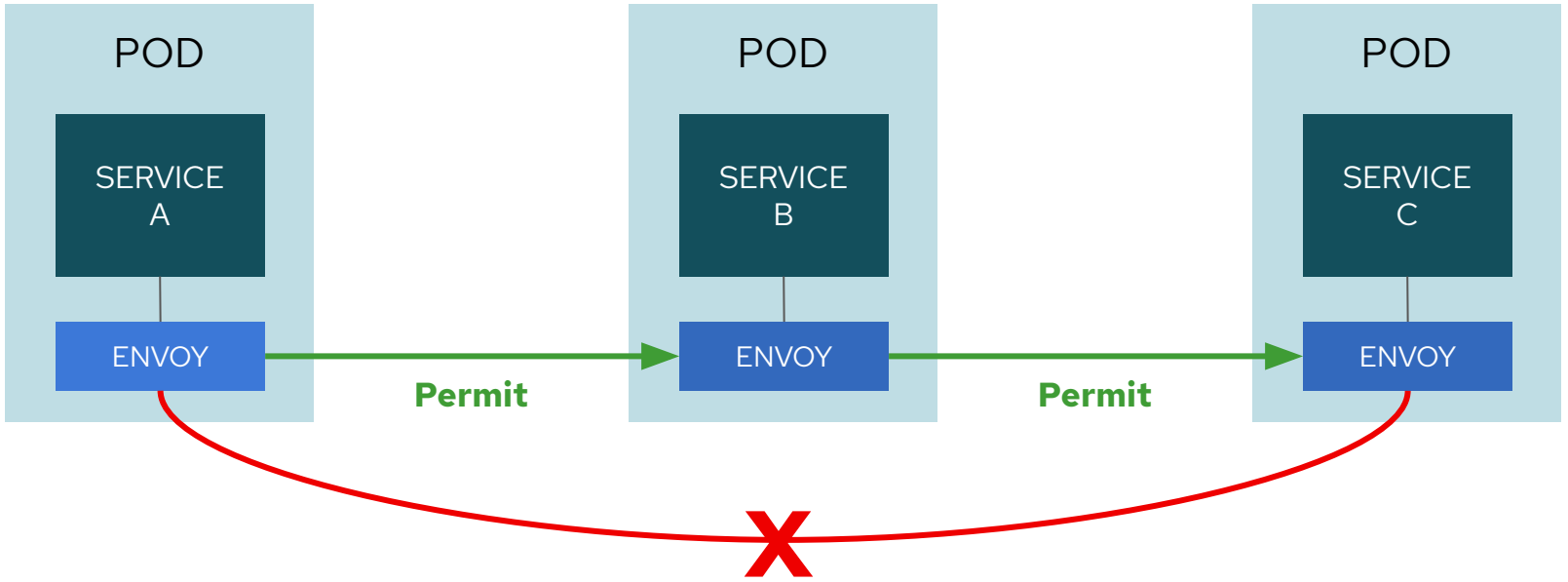
Rate limit



Red Hat

Sécuriser les applications avec Service Mesh

Contrôler le flow



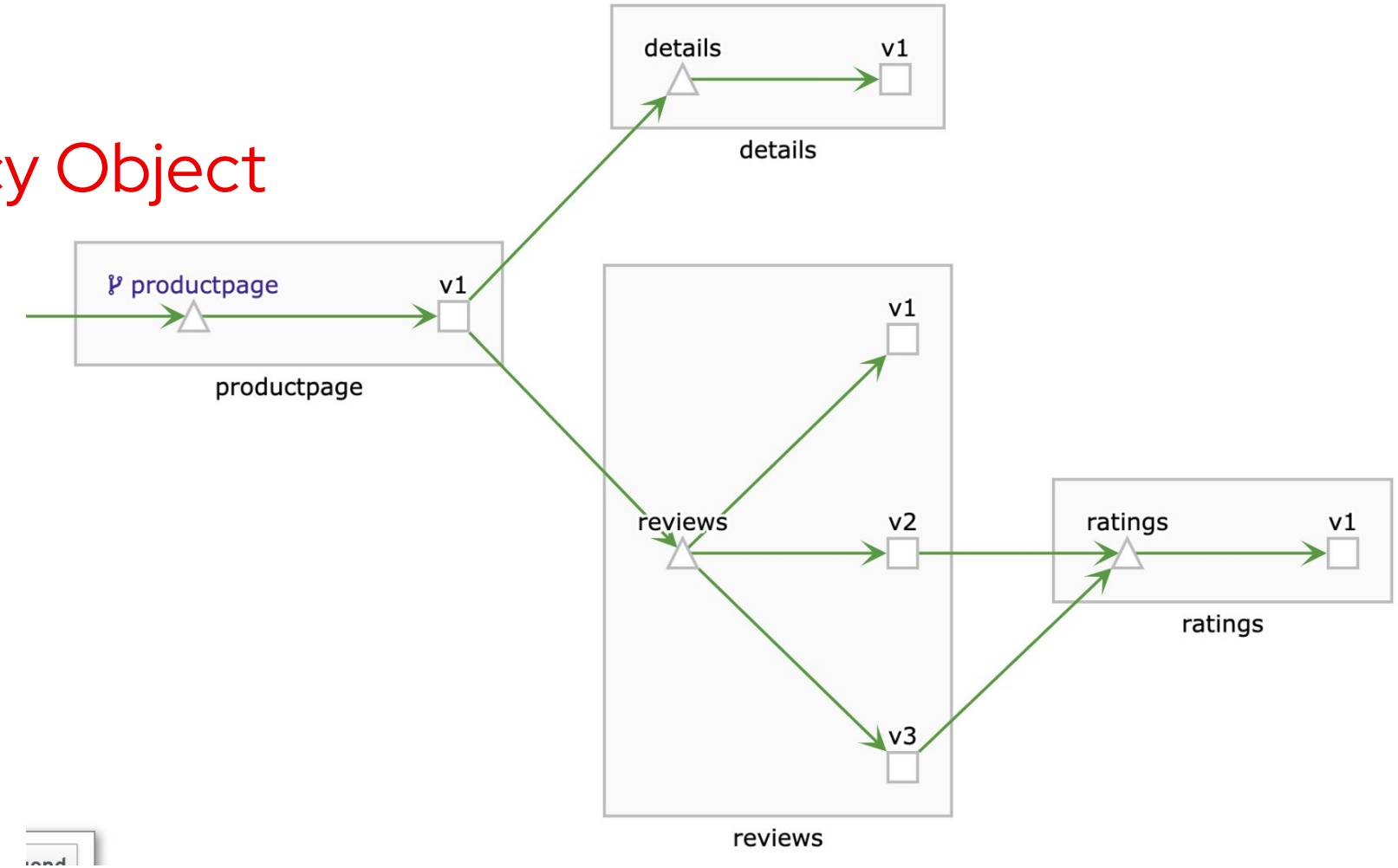
Red Hat

Démo

Network Policy Object

Démo

Network Policy Object



Merci

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat