

Remplacer un routeur par un serveur Linux

Retour d'expérience des passerelles d'accès à Grid'5000

David Loup

INRIA Rhône-Alpes, Laboratoire de l'Informatique du Parallélisme (LIP), Lyon

Dimitri Delabroye

INRIA Lille Nord Europe

Simon Delamare

CNRS, Laboratoire de l'Informatique du Parallélisme (LIP) , Lyon

Lucas Nussbaum

Université de Lorraine, LORIA



Introduction

- La plateforme Grid'5000

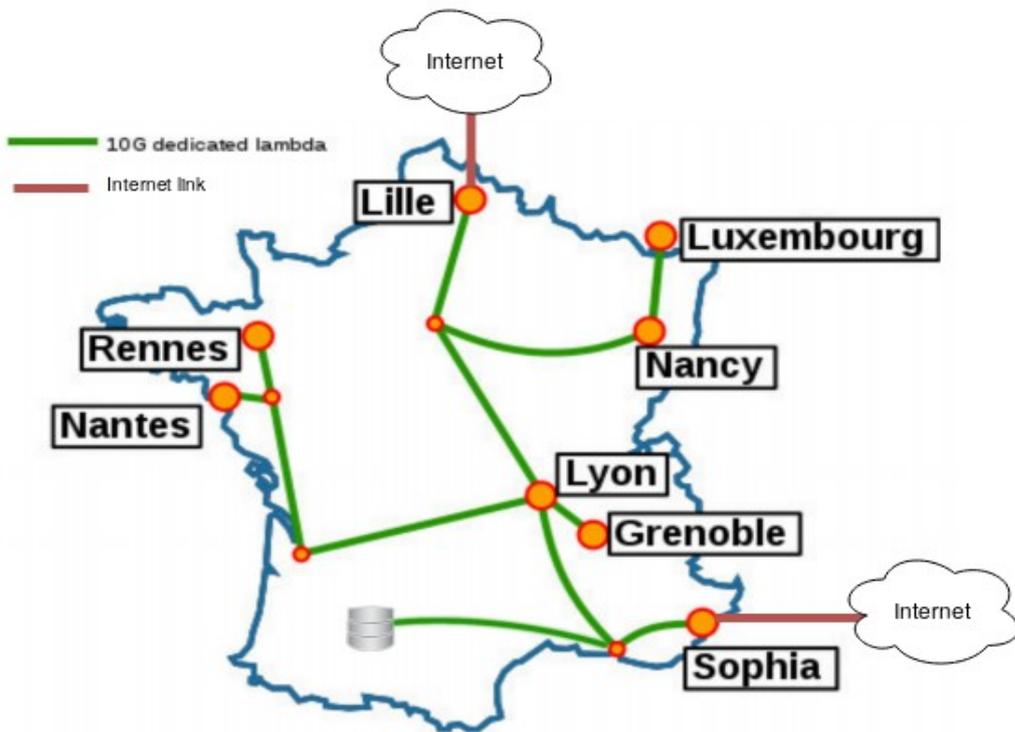
- La plateforme Grid'5000
- Solution historique

- La plateforme Grid'5000
- Solution historique
- Choix d'un serveur Linux

- La plateforme Grid'5000
- Solution historique
- Choix d'un serveur Linux
- Mise en œuvre
 - Configuration réseau finale
 - Intégration à l'infrastructure
 - Services spécifiques G5K
 - Performances

- La plateforme Grid'5000
- Solution historique
- Choix d'un serveur Linux
- Mise en œuvre
 - Configuration réseau finale
 - Intégration à l'infrastructure
 - Services spécifiques G5K
 - Performances
- Conclusion

La plateforme Grid'5000



- Plateforme d'expérimentation pour la recherche en informatique distribuée (HPC, Cloud, Big data, ...)
- Nœuds à disposition des chercheurs, entièrement reconfigurables
- 34 Clusters, ~900 nœuds, ~15 000 cores CPU
- 8 sites en France et au Luxembourg
- Cœur de réseau 10 Gbit/s Renater
- ~ 500 utilisateurs

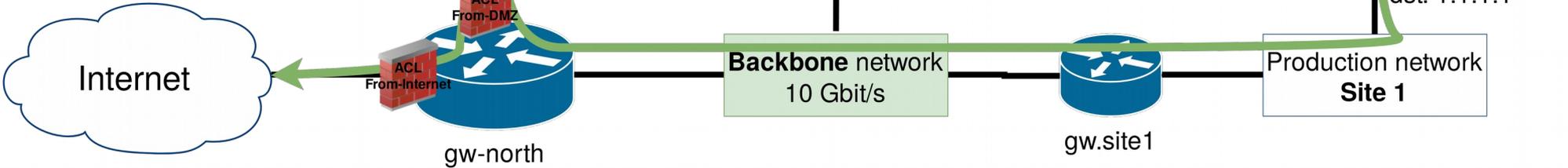
Solution historique

DMZ

- intranet
- ssh gateway
- API
- DNS



src : 194.254.60.35
dst: 1.1.1.1



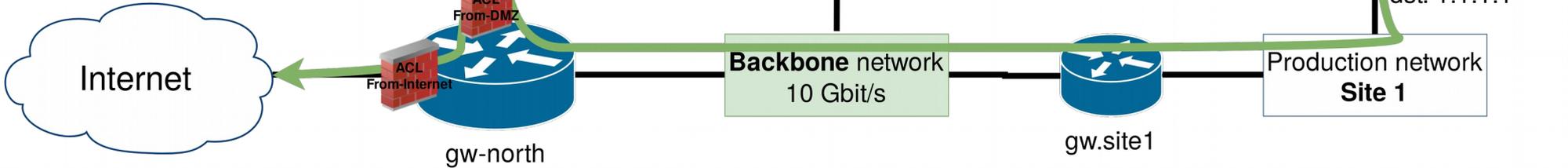
Solution historique

DMZ

- intranet
- ssh gateway
- API
- DNS

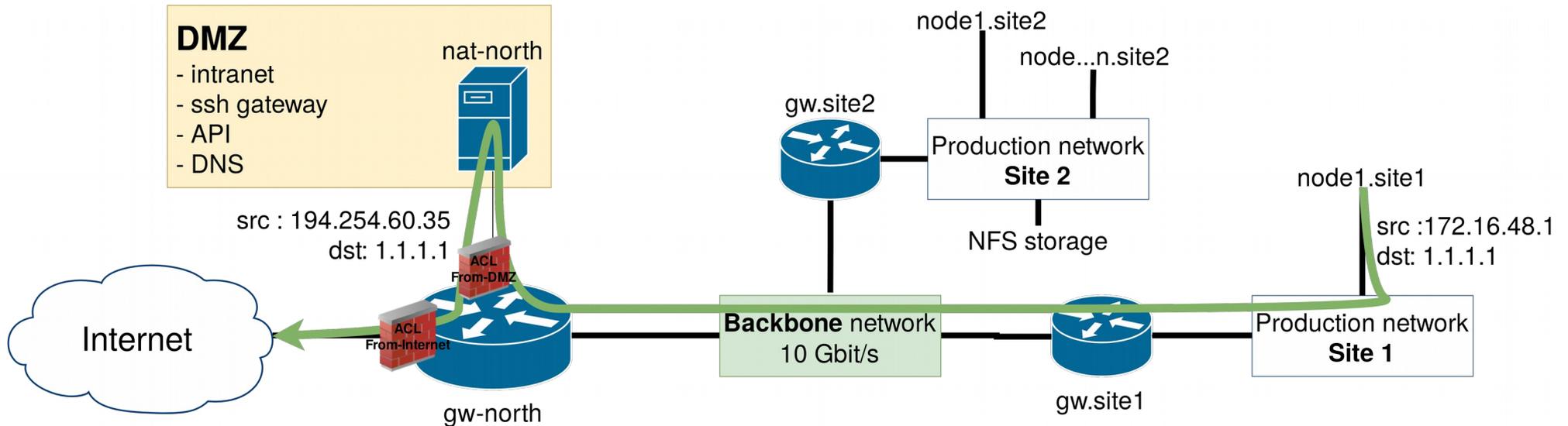


src : 194.254.60.35
dst: 1.1.1.1



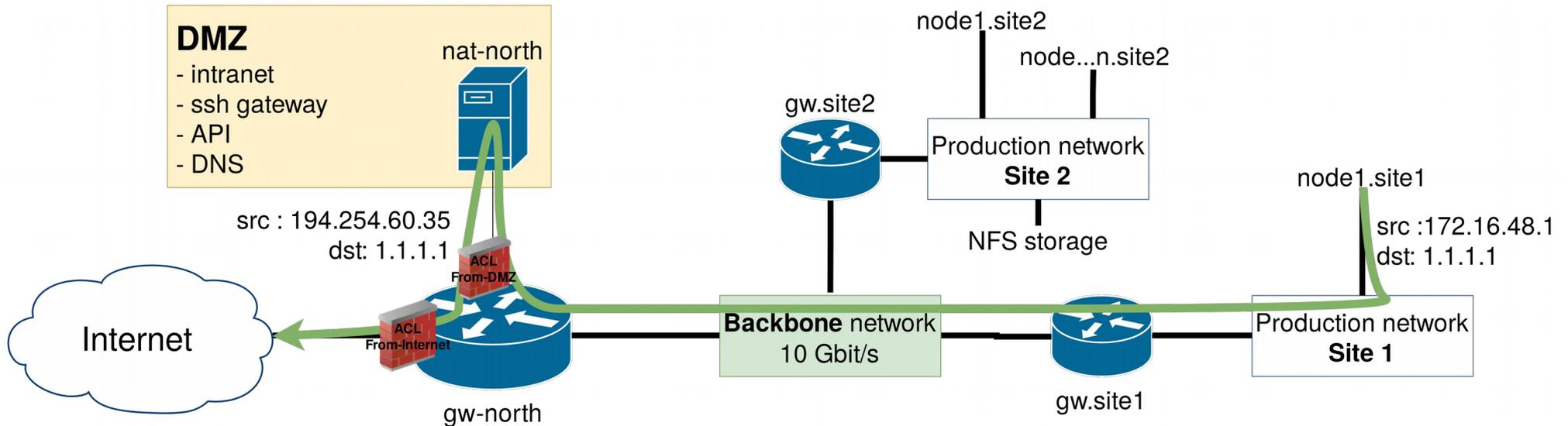
- 1 routeur par site

Solution historique



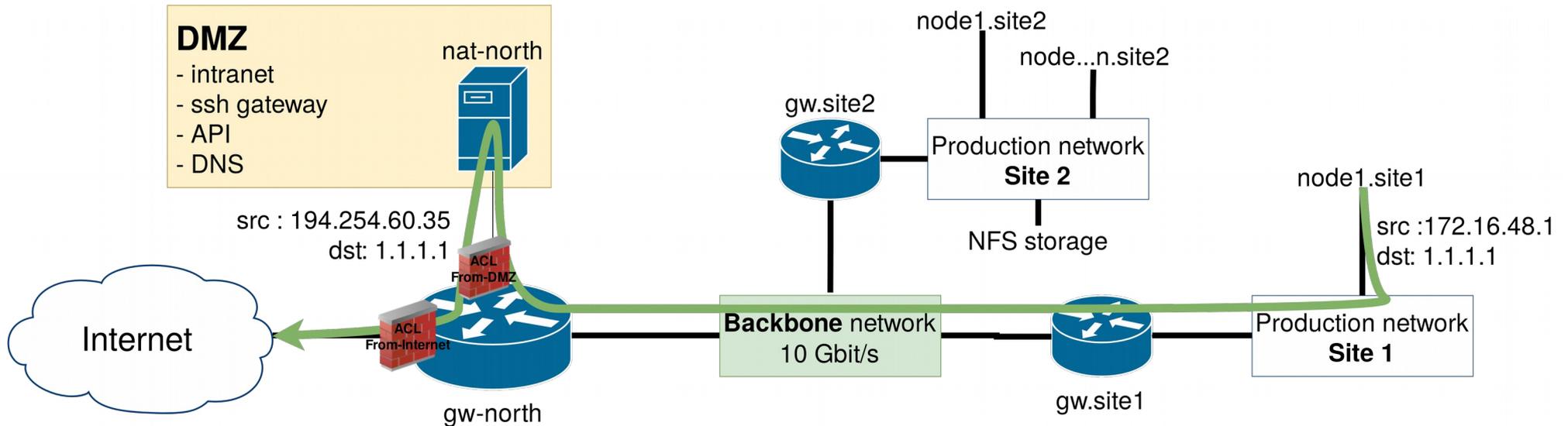
- 1 routeur par site
- 2 routeurs Cisco 2911 à Lille et Sophia
 - Internet, Backbone, DMZ
 - Routage : BGP, OSPF
 - Filtrage : ACL

Solution historique



- 1 routeur par site
- 2 routeurs Cisco 2911 à Lille et Sophia
 - Internet, Backbone, DMZ
 - Routage : BGP, OSPF
 - Filtrage : ACL
- 1 VM en DMZ
 - Proxy
 - Trace des connexions
 - Traduction d'adresses (NAT)

Solution historique



- 1 routeur par site
- 2 routeurs Cisco 2911 à Lille et Sophia
 - Internet, Backbone, DMZ
 - Routage : BGP, OSPF
 - Filtrage : ACL

- 1 VM en DMZ
 - Proxy
 - Trace des connexions
 - Traduction d'adresses (NAT)

Inconvénients :

- Administration manuelle
- Faibles débits: 120 Mbit/s

Choix d'un serveur Linux

Principales motivations :

- Nécessité d'intégrer des services supplémentaires
- Intégration du serveur à
 - Puppet : Gestion de la configuration
 - Icinga, Munin : Supervision
- Pas de fonctionnalités bloquées par licence
- Commandes Linux vs propriétaire

Choix d'un serveur Linux

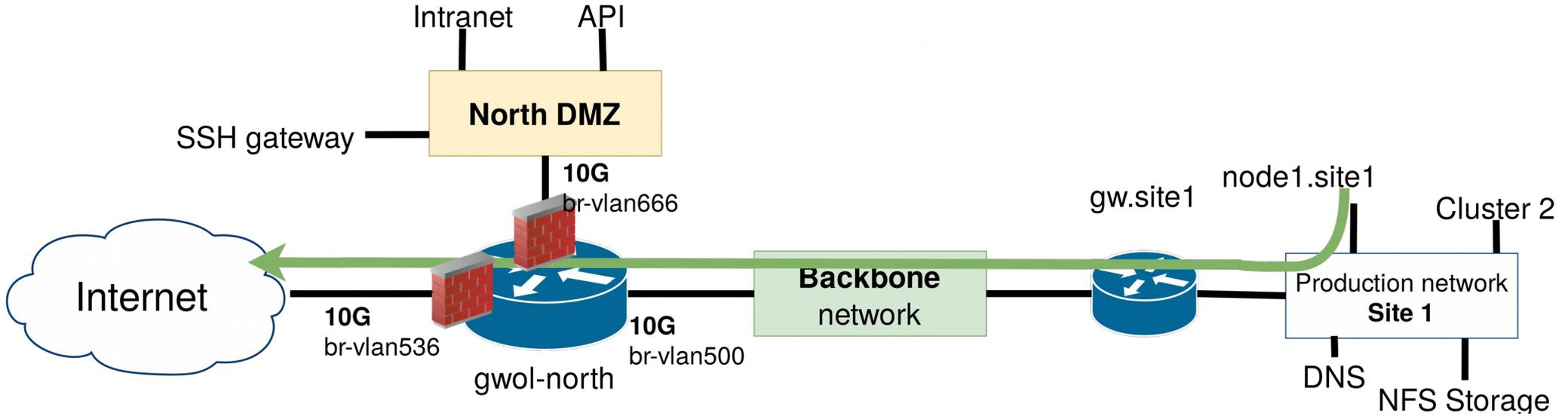
Principales motivations :

- Nécessité d'intégrer des services supplémentaires
- Intégration du serveur à
 - Puppet : Gestion de la configuration
 - Icinga, Munin : Supervision
- Pas de fonctionnalités bloquées par licence
- Commandes Linux vs propriétaire

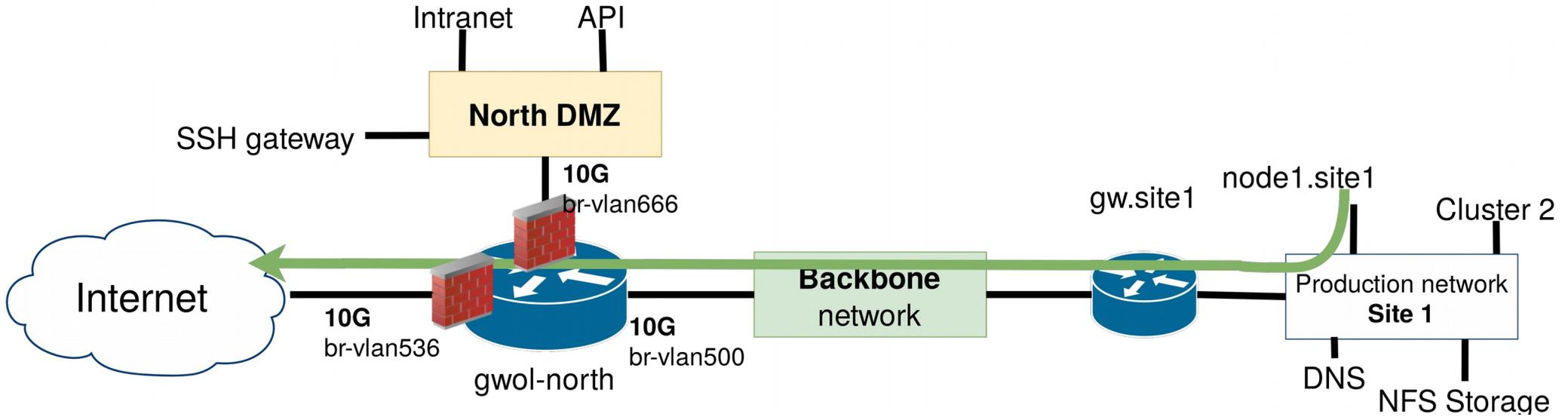
Dell PowerEdge R640

- 1 CPU Intel Xeon Gold 5122 3.6Ghz
 - 1 Intel 2P X710/2P I350 + 1 Intel X710
 - 4 Ports 10G SFP+
 - 2 Port 1G RJ45
 - 32 Go DDR4
 - 2 x SSD 450Go 6 Gbits/s
- ~ 3 000 €

Configuration réseau finale



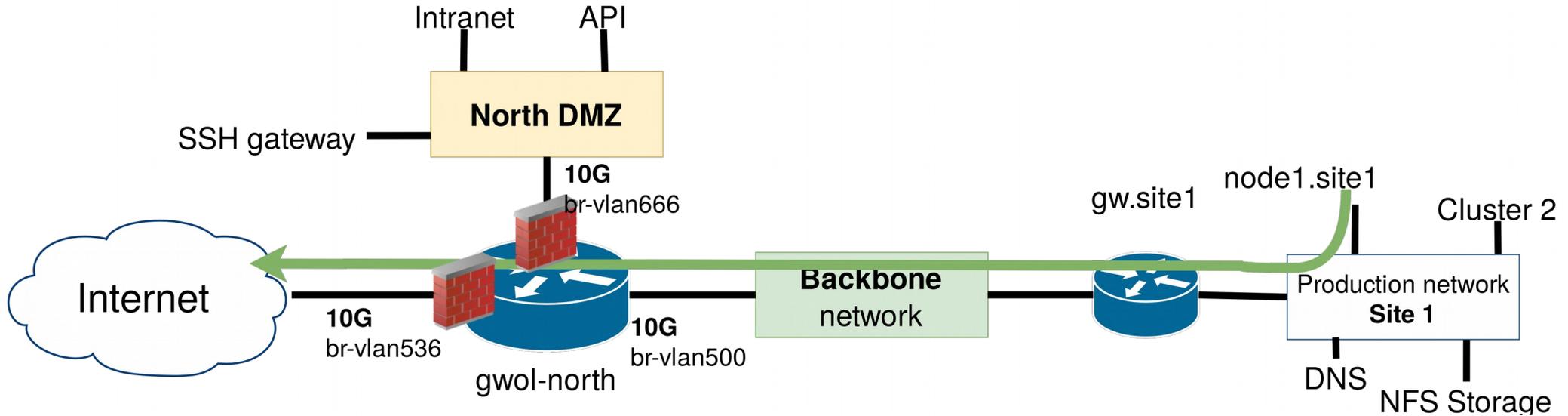
Configuration réseau finale



Vlans

- bridge-utils, vlans
- 3 bridges, 3 vlans

Configuration réseau finale



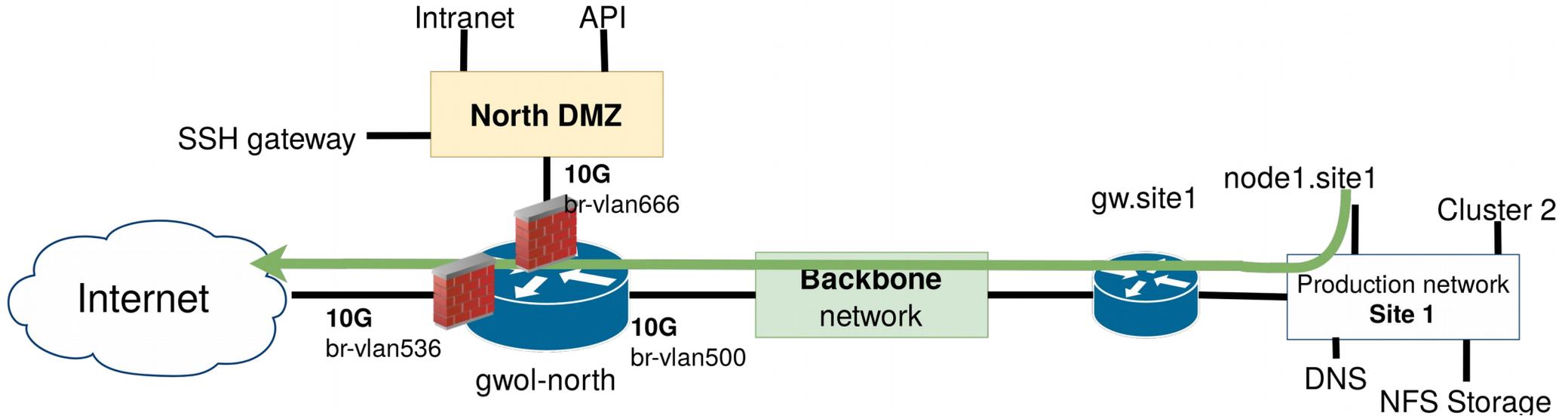
Vlans

- bridge-utils, vlans
- 3 bridges, 3 vlans

Filtrage

- Iptables
 - ~ 200 Règles
 - NAT
 - Trace du trafic

Configuration réseau finale



Vlans

- bridge-utils, vlans
- 3 bridges, 3 vlans

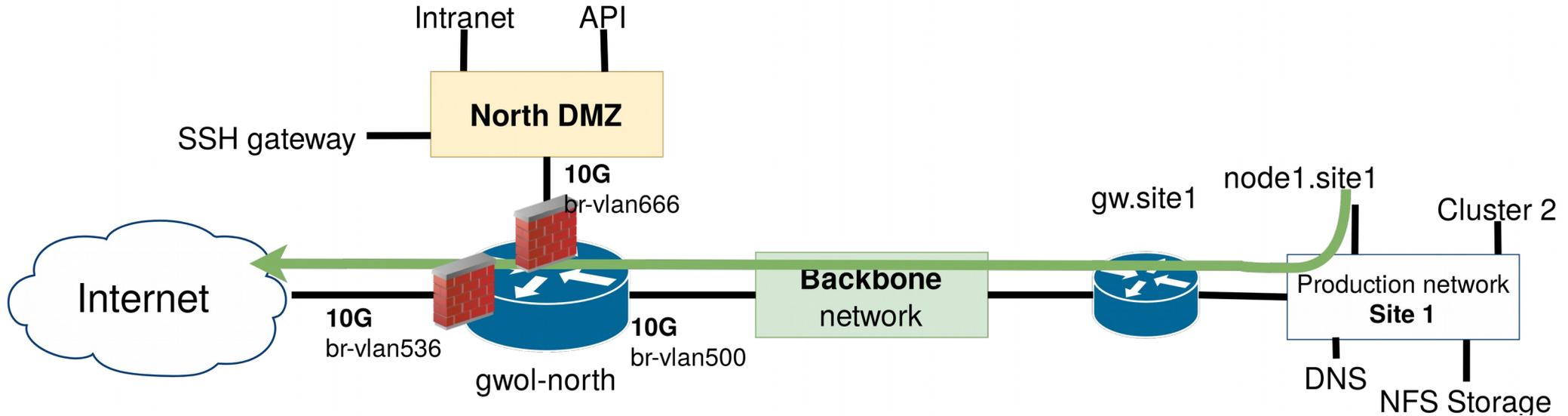
Filtrage

- Iptables
 - ~ 200 Règles
 - NAT
 - Trace du trafic

Routage dynamique

- FRR
 - ~ 50 routes
 - 11 voisins OSPF
 - 1 voisin BGP

Configuration réseau finale



Vlans

- bridge-utils, vlans
- 3 bridges, 3 vlans

Filtrage

- Iptables
 - ~ 200 Règles
 - NAT
 - Trace du trafic

Routage dynamique

- FRR
 - ~ 50 routes
 - 11 voisins OSPF
 - 1 voisin BGP

Proxy Cache

- Squid
- Iptables
 - proxy transparent

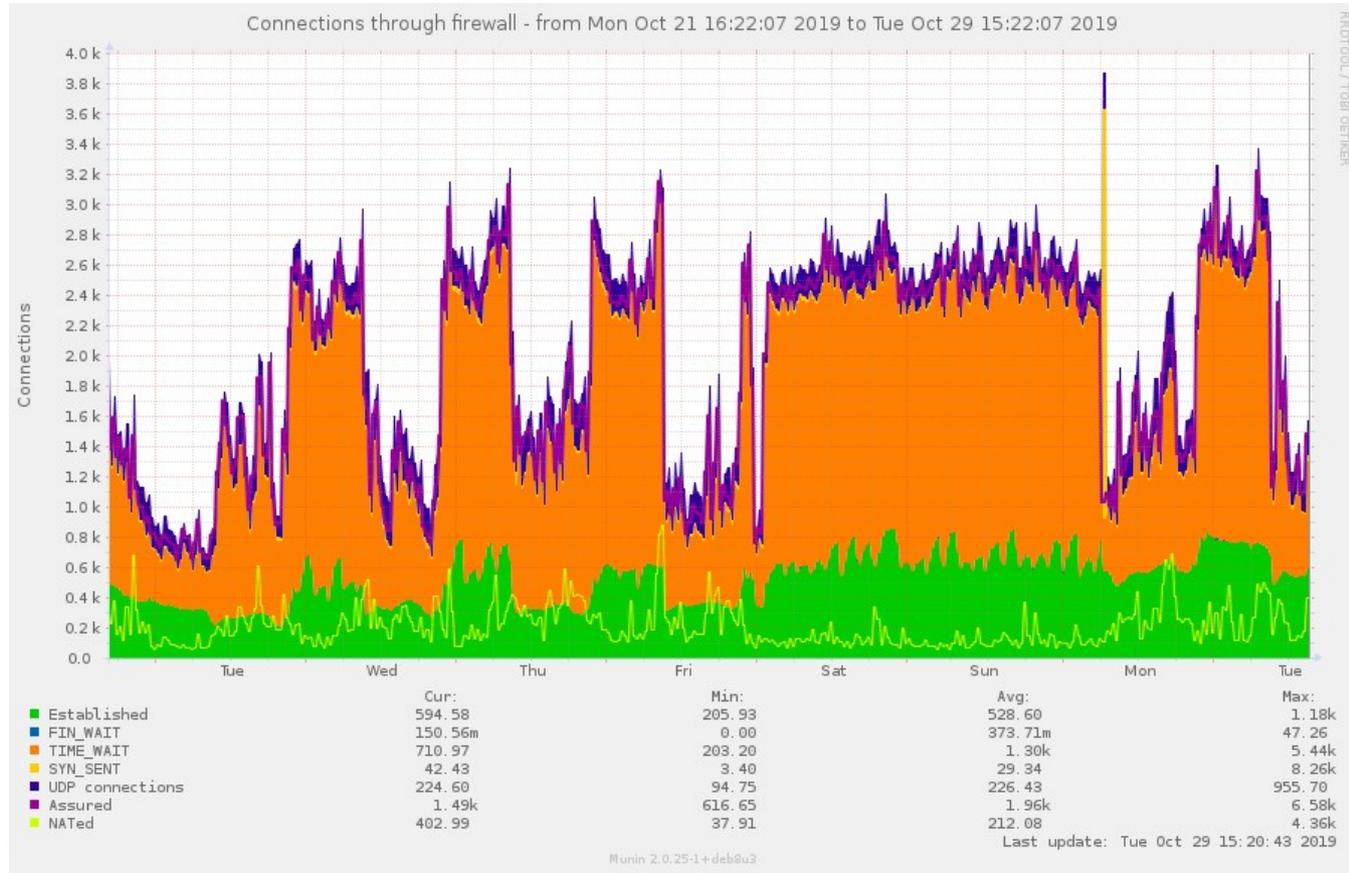
Puppet

- Gestion de la configuration de nos serveurs
 - Configurations précédentes gérées avec Puppet
 - Configuration versionnée
- Utilisation de templates et paramètres
 - Majeure partie de la configuration nord / sud identique
 - Différences nord / sud sous forme de paramètres dans les templates

```
router bgp <%= bgp['local_as'] %>
  bgp log-neighbor-changes
  network <%= bgp['primary'] %> mask <%= bgp['primary_mask']%> route-map Primary-BGP
  network <%= bgp['secondary'] %> mask <%= bgp['secondary_mask'] %> route-map Secondary-BGP
  neighbor <%= bgp['neighbor'] %> remote-as <%= bgp['remote_as'] %>
  neighbor <%= bgp['neighbor'] %> password <%= bgp['pass'] %>
  neighbor <%= bgp['neighbor'] %> send-community
!
```

Supervision : Icinga et Munin

- États voisins BGP, OSPF
- Taille cache Squid
- Disque, CPU, mémoire



Services spécifiques G5K

Des fonctionnalités « sur mesure » :

Services spécifiques G5K

Des fonctionnalités « sur mesure » :

- Proxy transparent directement sur le routeur

Services spécifiques G5K

Des fonctionnalités « sur mesure » :

- Proxy transparent directement sur le routeur
- IPv6 : Projet de pare-feu configurable par les utilisateurs

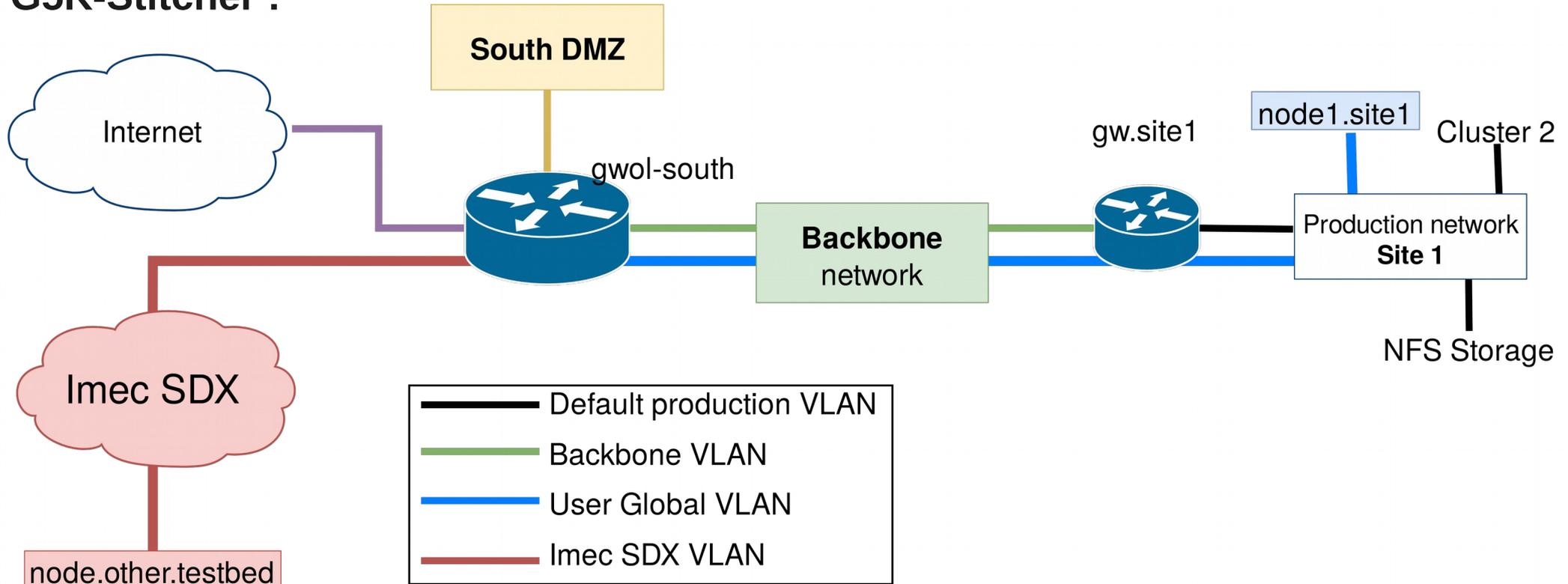
Services spécifiques G5K

Des fonctionnalités « sur mesure » :

- Proxy transparent directement sur le routeur
- IPv6 : Projet de pare-feu configurable par les utilisateurs
- **G5K-Stitcher**
 - Service logiciel pour interconnecter dynamiquement des vlans internes et externes
 - Permet la connexion entre Grid'5000 et une autre plateforme (via I Mec SDX)

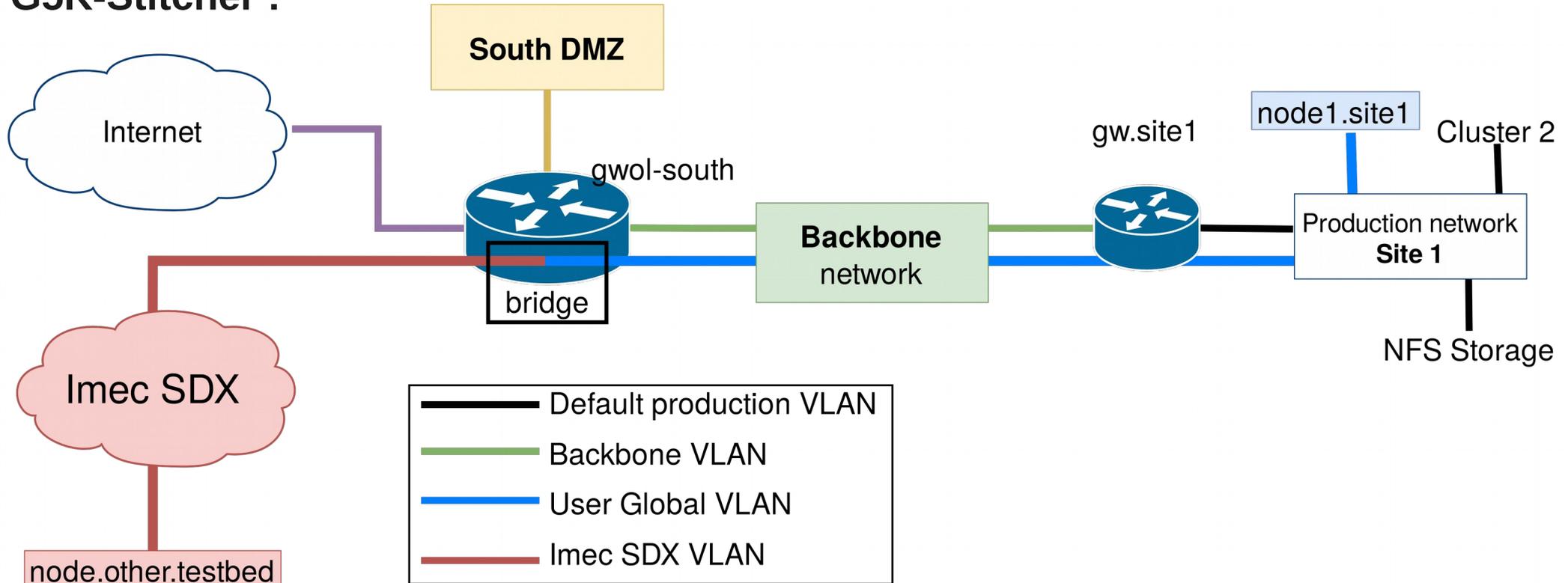
Services spécifiques G5K

G5K-Stitcher :



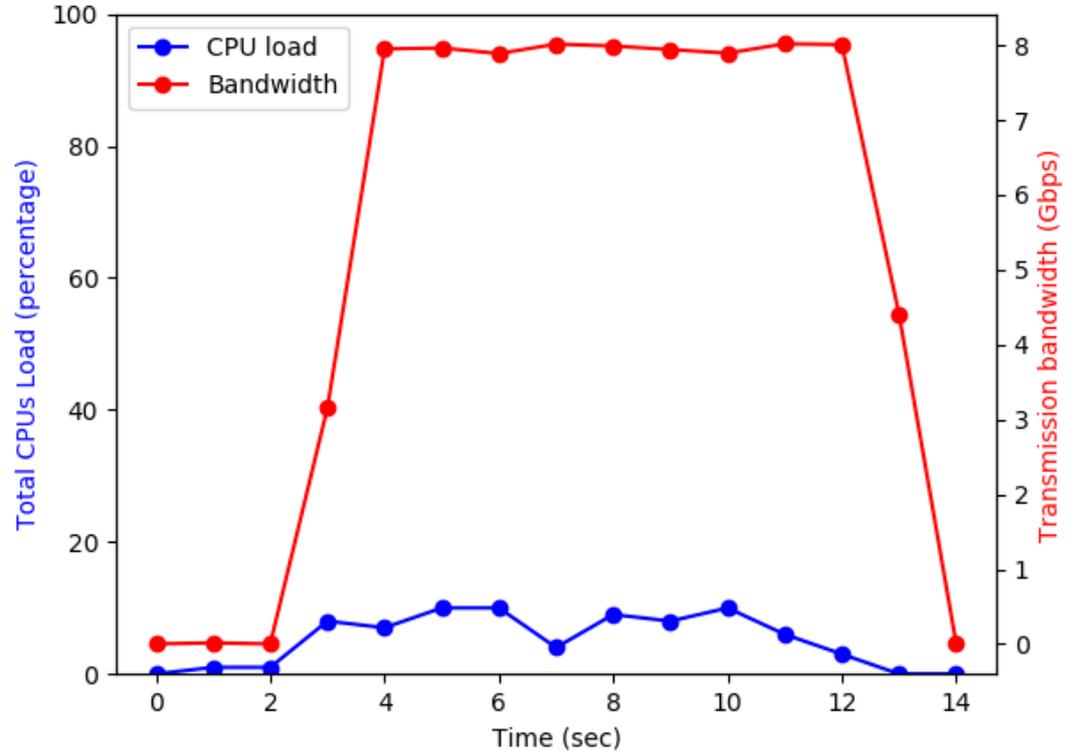
Services spécifiques G5K

G5K-Stitcher :



Performances

- ~ 10 Gbit/s vers Internet
- 10 Gbit/s vers le cache
- Filtrage : faible impact sur le CPU, pas d'impact sur le débit.



Conclusion



Conclusion

- Utilisation d'un serveur Linux comme routeur pour
 - Simplifier l'administration de notre infrastructure réseau
 - Intégrer des services qu'on ne peut pas déployer sur des routeurs dédiés

Conclusion

- Utilisation d'un serveur Linux comme routeur pour
 - Simplifier l'administration de notre infrastructure réseau
 - Intégrer des services qu'on ne peut pas déployer sur des routeurs dédiés
- Configuration
 - Serveur R640 ~ 3 000€
 - 3 ports 10 Gbit/s
 - 200 règles de filtrages
 - 50 routes

Conclusion

- Utilisation d'un serveur Linux comme routeur pour
 - Simplifier l'administration de notre infrastructure réseau
 - Intégrer des services qu'on ne peut pas déployer sur des routeurs dédiés
- Configuration
 - Serveur R640 ~ 3 000€
 - 3 ports 10 Gbit/s
 - 200 règles de filtrages
 - 50 routes
- Perspectives
 - White box switch (Cumulus OS, OPX) : Avantages Linux + matériel réseaux dédiés

Merci !

Des questions ?

