

Migration des pare-feu Internet de l'Université de Rennes 1 sous OpenBSD / Packet-Filter

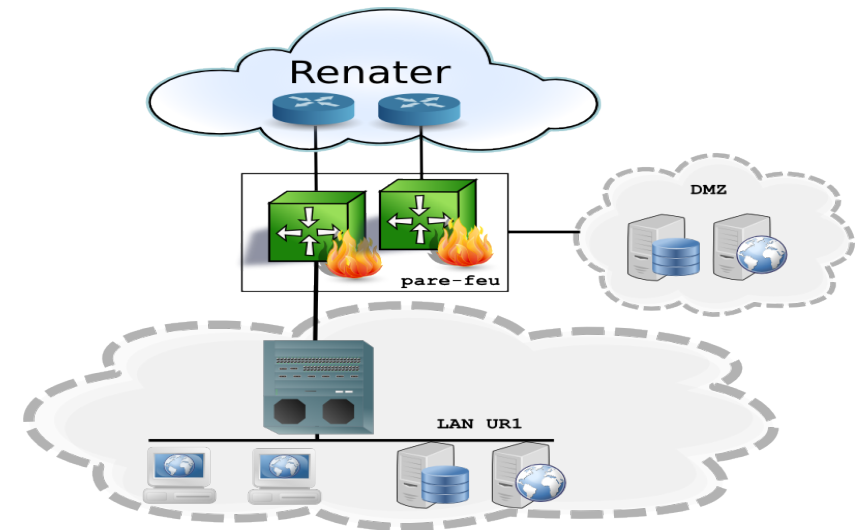
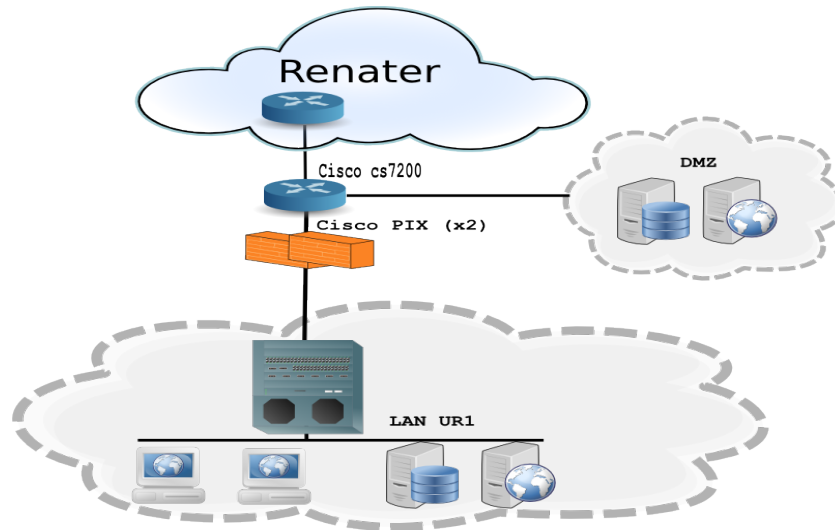
Patrick Lamaizière

Direction du Système d'Information

Université de Rennes 1

Introduction

- Connexion internet via un routeur Cisco 7204 et deux pare-feu PIX
- Performances insuffisantes, plafonnement à 200 Mbits/s
- Remplacement par deux pare-feu utilisant du matériel standard (x86) sous OpenBSD



OpenBSD / Packet Filter

■ OpenBSD

- Système libre de type Unix dérivé de 4.4 BSD

■ Packet Filter

- Pare-feu à états : lorsqu'une règle autorise un paquet, un état est automatiquement créé qui autorise les paquets suivants et les paquets retours
 - Simplifie les règles (pas besoin de gérer les paquets retours)
 - Améliore les performances
- PF n'est pas un pare-feu applicatif

■ Common address redundancy protocol (CARP)

- Partage d'une IP virtuelle entre plusieurs machines d'un même sous réseau
- Permet la redondance entre plusieurs machines

■ Pfsync(4)

- synchronisation des états entre plusieurs pare-feu

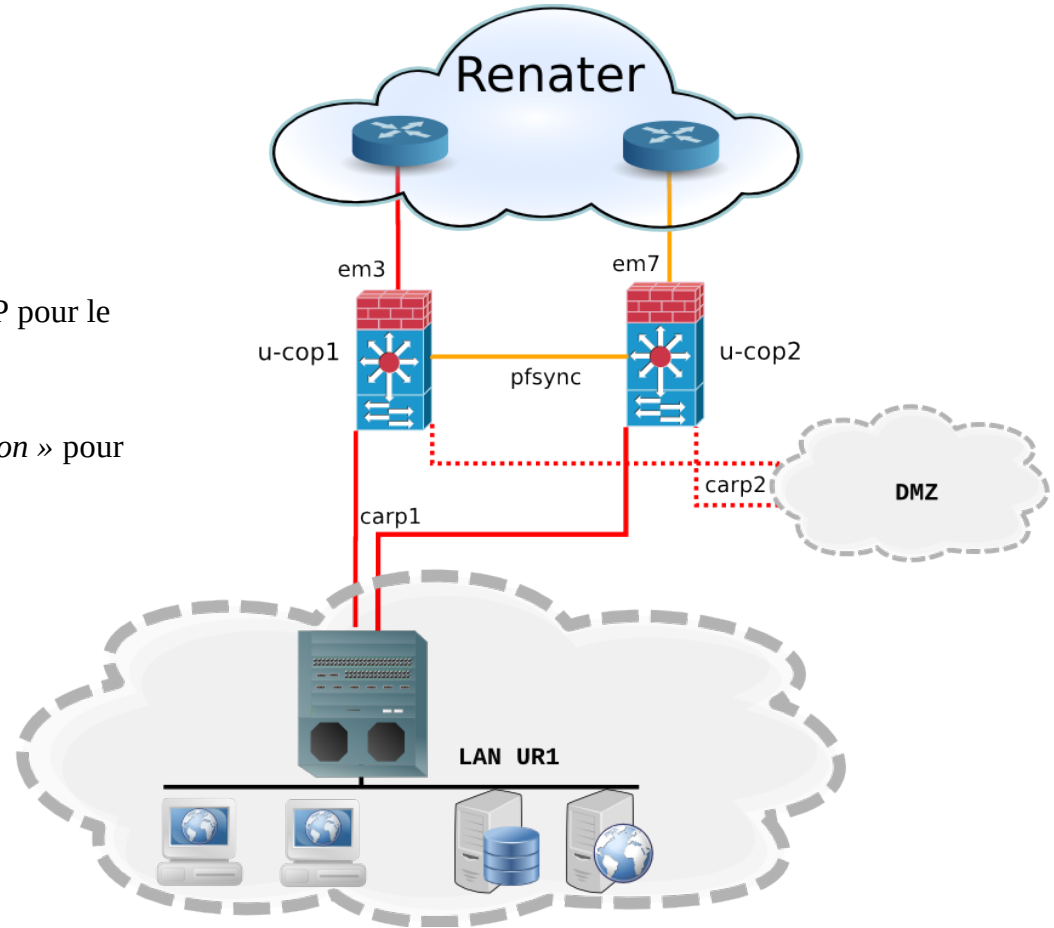
Mise en œuvre

■ Architecture :

- Double attachement avec Renater
- Configuration asymétrique

■ Redondance

- Utilisation des communautés BGP pour le routage coté Renater
- CARP sur les interfaces internes
- ifstated(8) « *Interface State daemon* » pour la synchronisation BGP/CARP



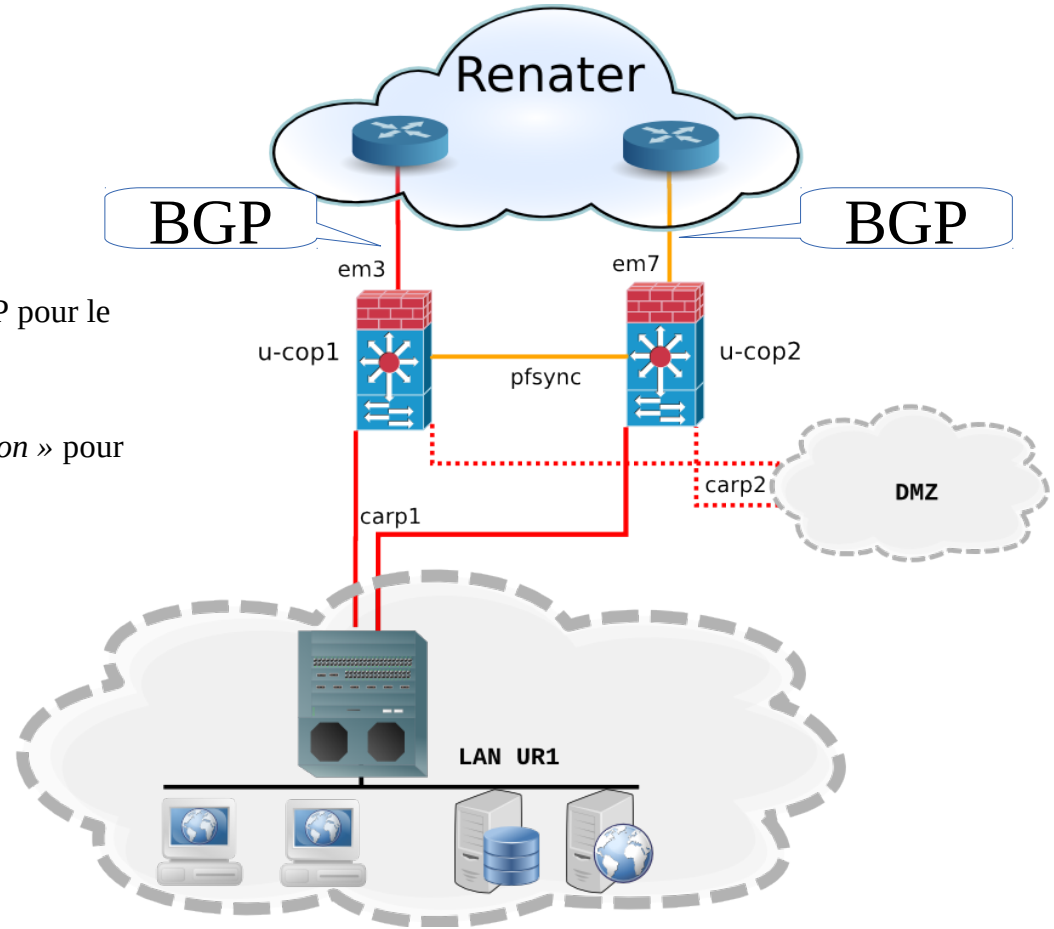
Mise en œuvre

■ Architecture :

- Double attachement avec Renater
- Configuration asymétrique

■ Redondance

- Utilisation des communautés BGP pour le routage coté Renater
- CARP sur les interfaces internes
- ifstated(8) « *Interface State daemon* » pour la synchronisation BGP/CARP



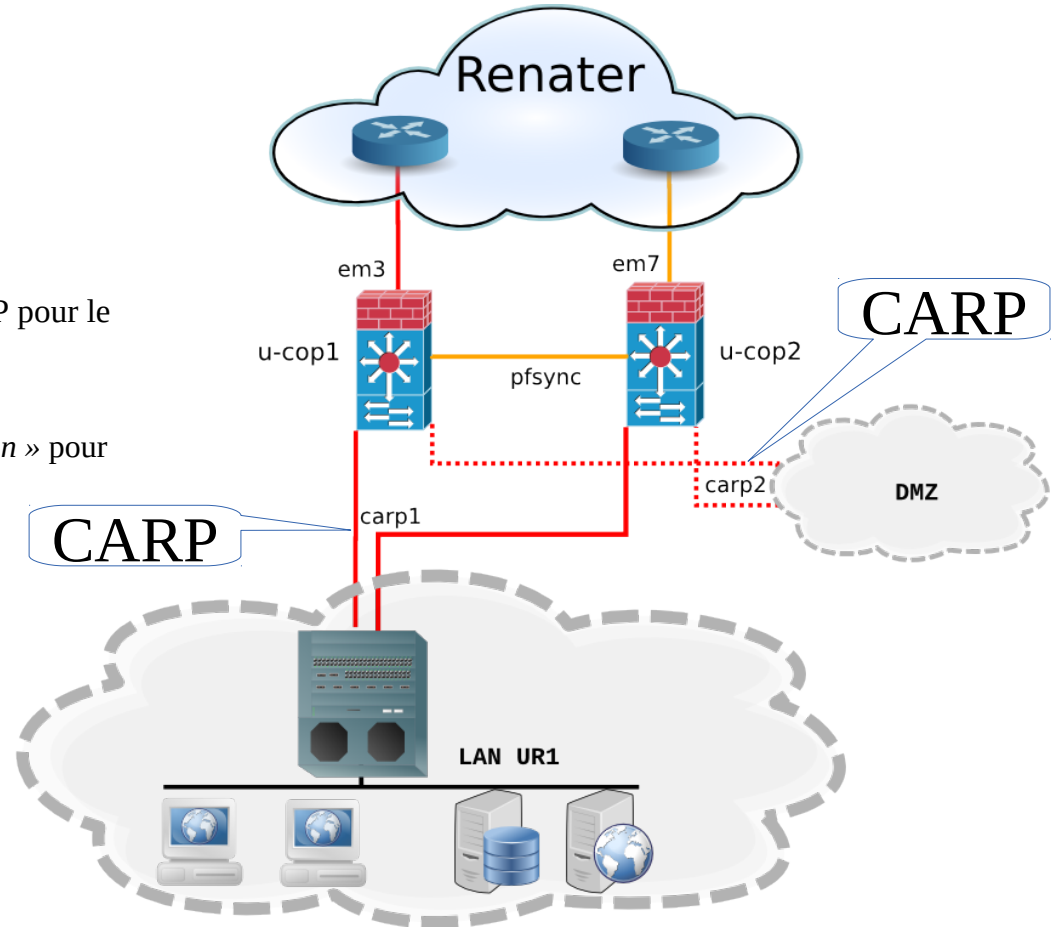
Mise en œuvre

■ Architecture :

- Double attachement avec Renater
- Configuration asymétrique

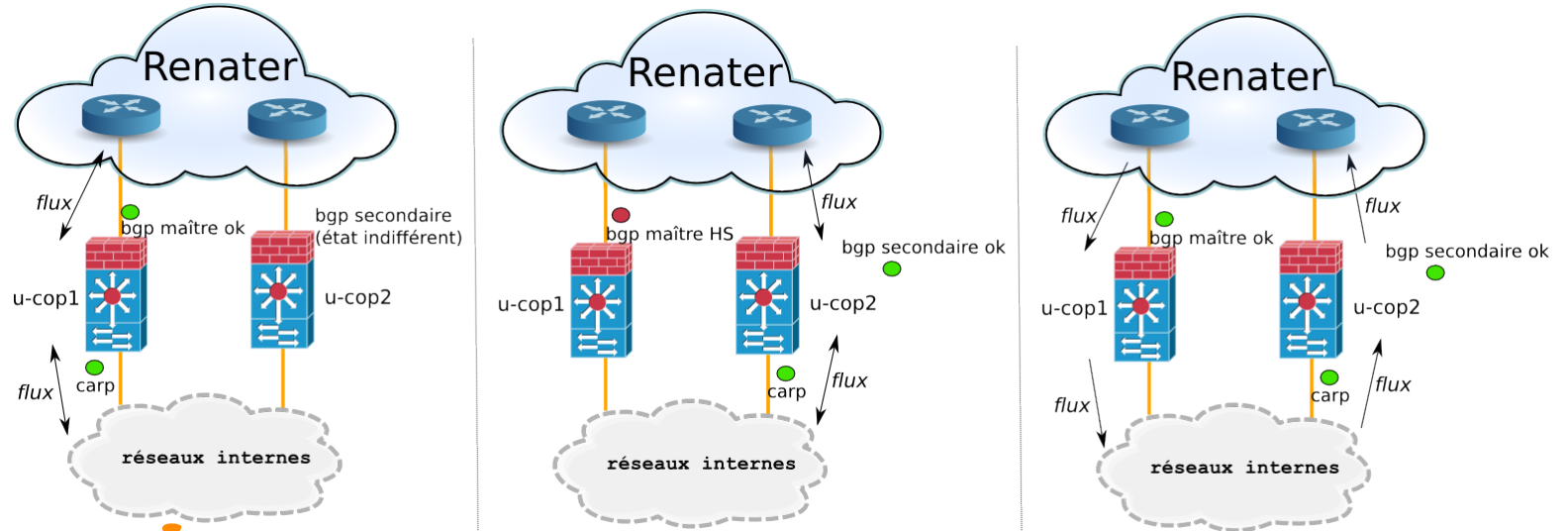
■ Redondance

- Utilisation des communautés BGP pour le routage coté Renater
- CARP sur les interfaces internes
- ifstated(8) « *Interface State daemon* » pour la synchronisation BGP/CARP



Redondance

- **Fonctionnement normal (u-cop1) /secours (u-cop2)**
- **Pas de retour automatique de u-cop2 vers u-cop1, nécessité d'une intervention humaine sur u-cop1**
- **Si problème sur u-cop1**
 - Ifstated le détecte et effectue deux actions : arrêt de bgpd et dégradation CARP
 - La dégradation CARP provoque le basculement sur u-cop2
- **Retour sur u-cop1 : démarrage de bgpd puis suppression de la dégradation CARP**



Métrologie

- **Sonde Netflow : pflow(4)**
- **Statistiques via net-snmpd**
 - Trafic, taux d'erreurs, nombre d'états ...
- **Surveillance via Cacti et Nagios**

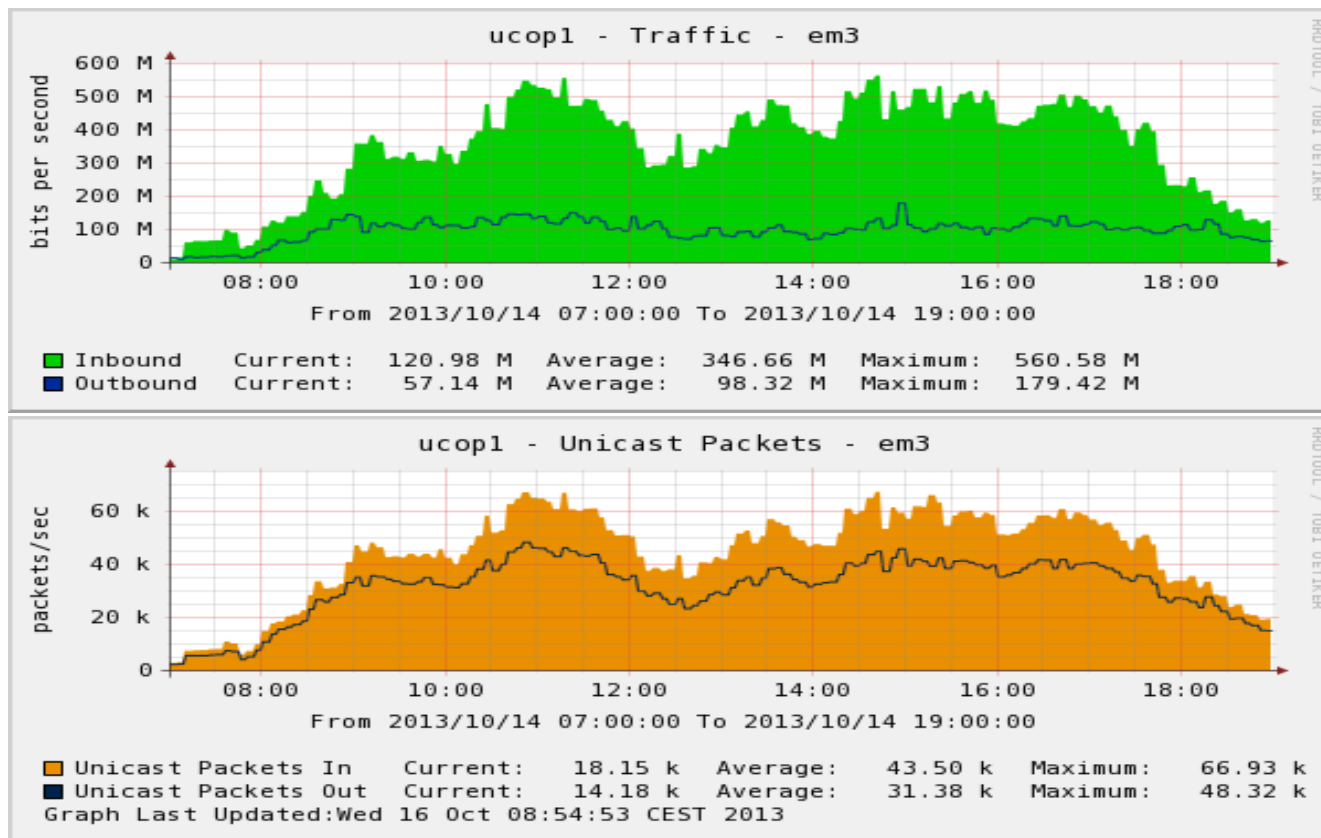
Performances

■ Serveur Dell R610

- Processeur Xeon 2,27 GHz
- Carte réseau intégrée Broadcom 4 ports Gbits cuivre
- Carte réseau Intel 4 ports Gbits cuivre
- Carte réseau Intel 4 ports Gbits fibre

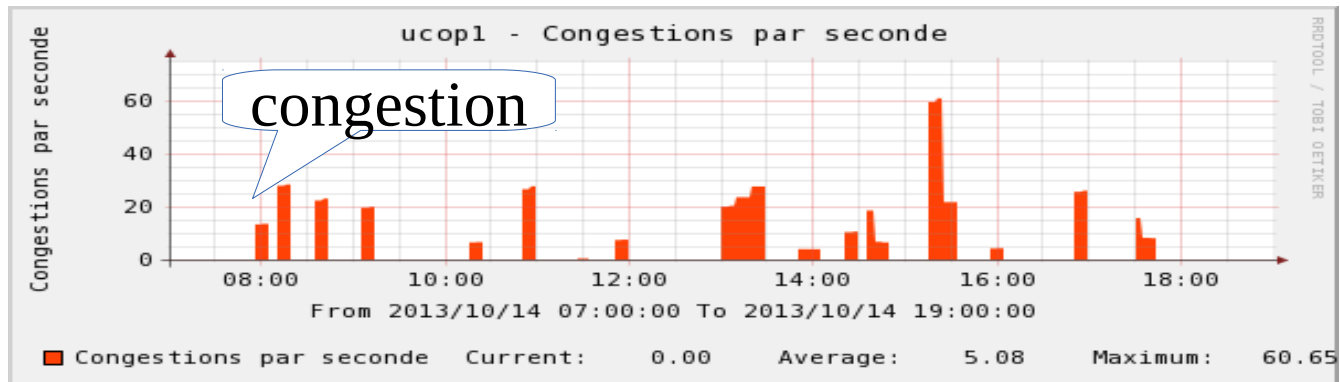
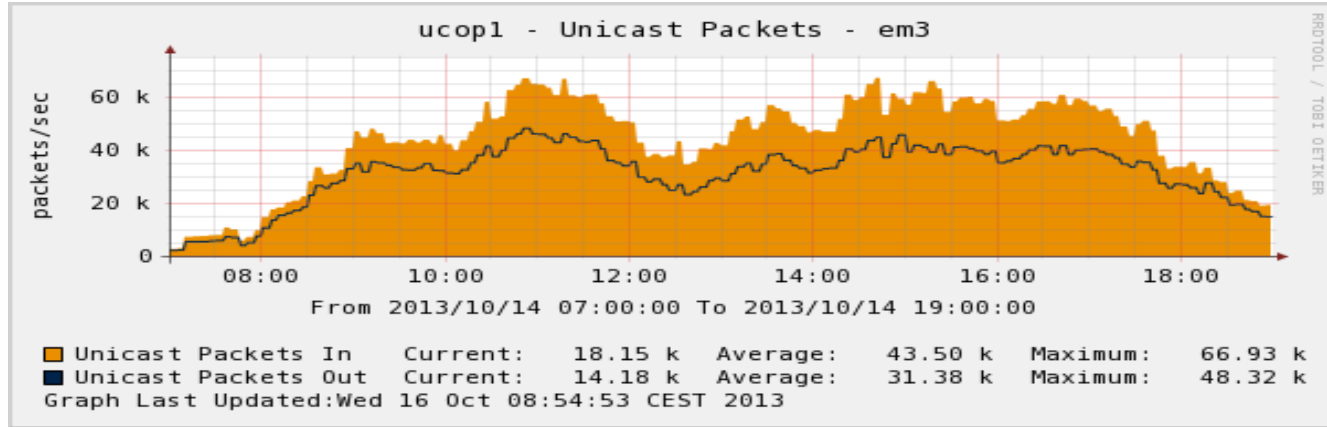
Performances

Traffic



Performances

Traffic / congestion



Conclusion

- **OpenBSD est une bonne solution pour des pare-feu redondants**
- **Robuste**
- **Mais on arrive en limite du système...**
- **Quelles solutions ?**
 - Matériel plus performant mais le noyau d'OpenBSD n'est pas SMP ce qui limite fortement les performances
 - FreeBSD, mais PF souffre d'un verrou global ce qui limite autant (sauf dans FreeBSD 10 mais version beta)
- **Des questions ?**