



www.cnrs.fr

Migration vers l'open-source de l'infrastructure de pare-feu du campus CNRS d'Orléans



PLAN

- Contexte
- Conduite du projet
- La solution mise en place
- Retour d'expérience
- Perspectives / Conclusions



Contexte

Conduite du projet

Solution mise en place

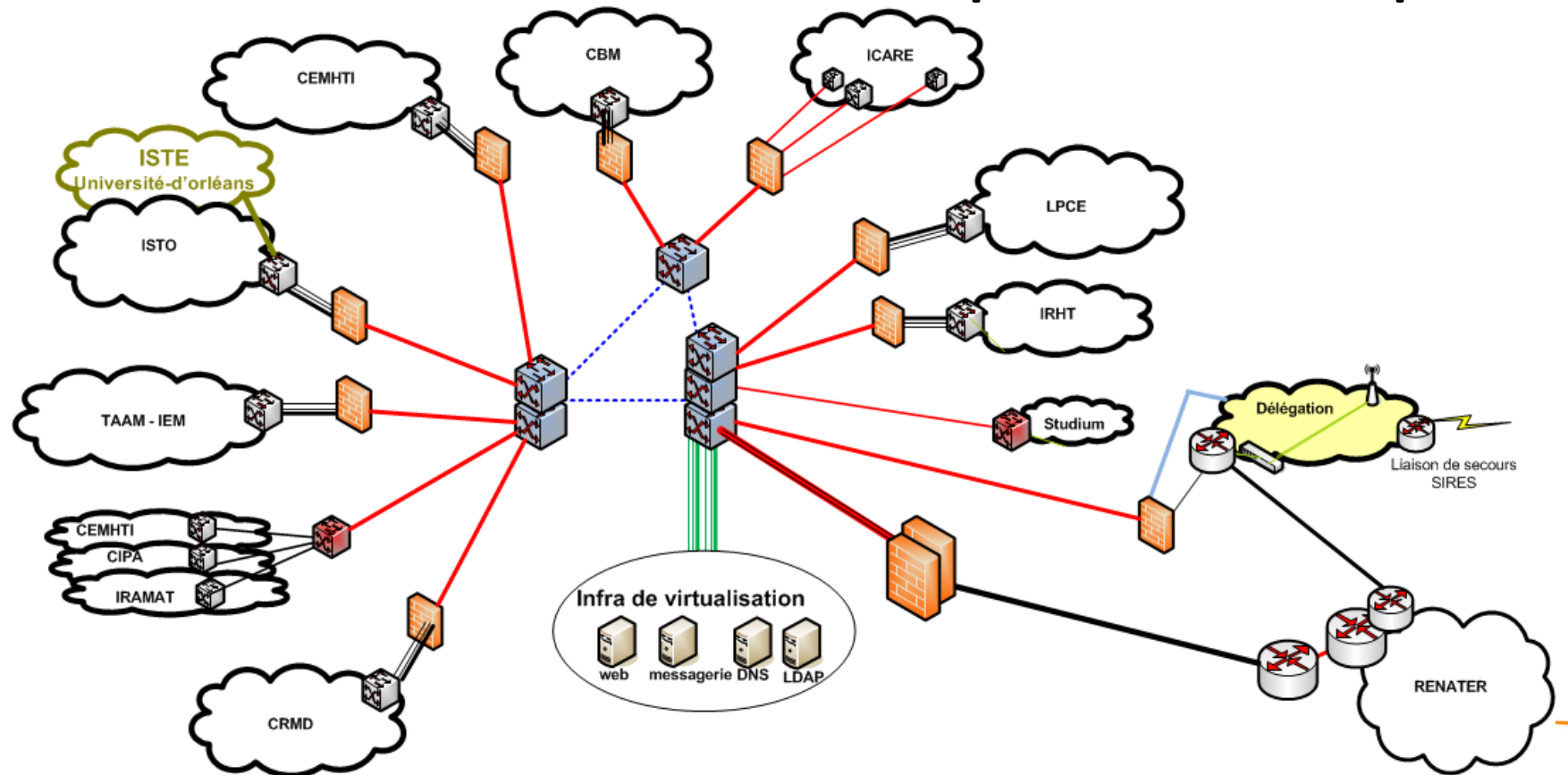
Retour d'expérience

Perspectives

Le campus CNRS d'Orléans



Présentation informatique du campus



Présentation du groupe de Travail

- Le GT est composé de cinq membres :
 - Laurent Catherine OSUC
 - Franck Elie LPC2E
 - Thomas Nodimar IRHT
 - François Vivet CEMHTI
 - Xavier Laure DCLPC
- Avec la participation active d'autres intervenants



La problématique et les objectifs

- Renouvellement des anciens pare-feu
 - Laboratoire : obligatoire car en fin de vie
 - Tête de campus : pas encore en fin de vie mais...
- Intégration d'IPv6 au niveau des laboratoires
- Valider la stratégie SSI des laboratoires
- Diminution des coûts de maintenance



Le besoin et les contraintes

- Limiter l'impact du changement sur les ASR
- Robustesse, performance
- Délégation d'administration
- Reprise sur arrêt de la production (H+2)



Contexte

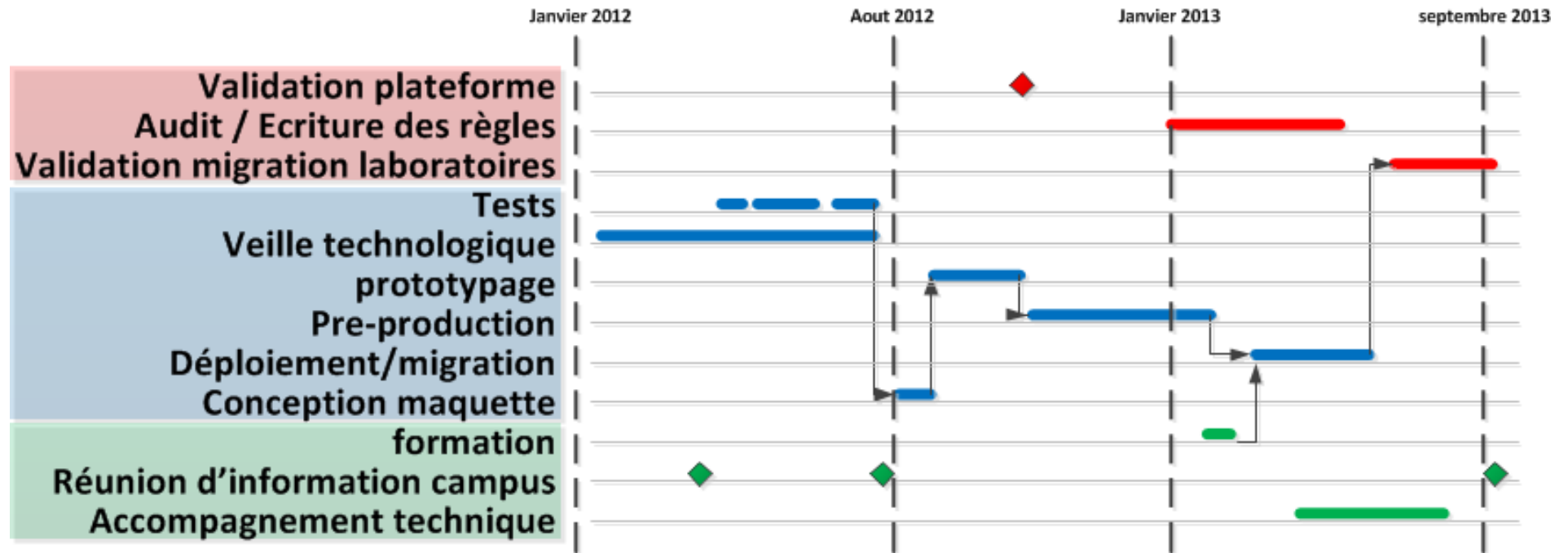
Conduite du projet

Solution mise en place

Retour d'expérience

Perspectives

Déroulement du projet



Critères de sélection

- Richesse des outils d'administration (délégation, gestion des log, monitoring, ...)
- Qualité de l'interface graphique
- Fonctionnalités du pare-feu:
 - existantes : IPsec, relai DHCP, NAT, OSPFv2, ...
 - nouvelles : IPv6 (OSPFv3)
- Performances du pare-feu (routage/nb interfaces)
- Pérennité matérielle / stratégies commerciales
- Evolutivité fonctionnelle



Contexte

Conduite du projet

Solution mise en place

Retour d'expérience

Perspectives

Critères de sélection

| Critères | « Notre » solution Open-source | Constructeur en place | Autres solutions commerciales |
|--------------------------------|--------------------------------|-----------------------|-------------------------------|
| IHM / ergonomie | ** | *** | **/** |
| Fonctionnalités du pare-feu | *** | ** (IPv6) | **/** |
| Outils d'administration | *** | ** | **/** |
| Performances/Prix | *** | ** | * |
| Pérennité/évolution | *** | * (stratégie) | * (stratégie) |
| facilité Intégration/migration | * | ***** | **/** |
| Facilité de prise en main ASR | ** | *** | ** |
| Coût achat & maintenance | ***** | ** | * |
| « confort » exploitation | * (support local) | *** | *** |

Critères de sélection

| Critères | « Notre » solution Open-source |
|--------------------------------|--------------------------------|
| IHM / ergonomie | ** |
| Fonctionnalités du pare-feu | *** |
| Outils d'administration | *** |
| Performances/Prix | *** |
| Pérennité/évolution | *** |
| facilité Intégration/migration | * |
| Facilité de prise en main ASR | ** |
| Coût achat & maintenance | ***** |
| « confort » exploitation | * (support local) |

Solution retenue :

Filtrage

Netfilter/Iptables

IHM de gestion des règles

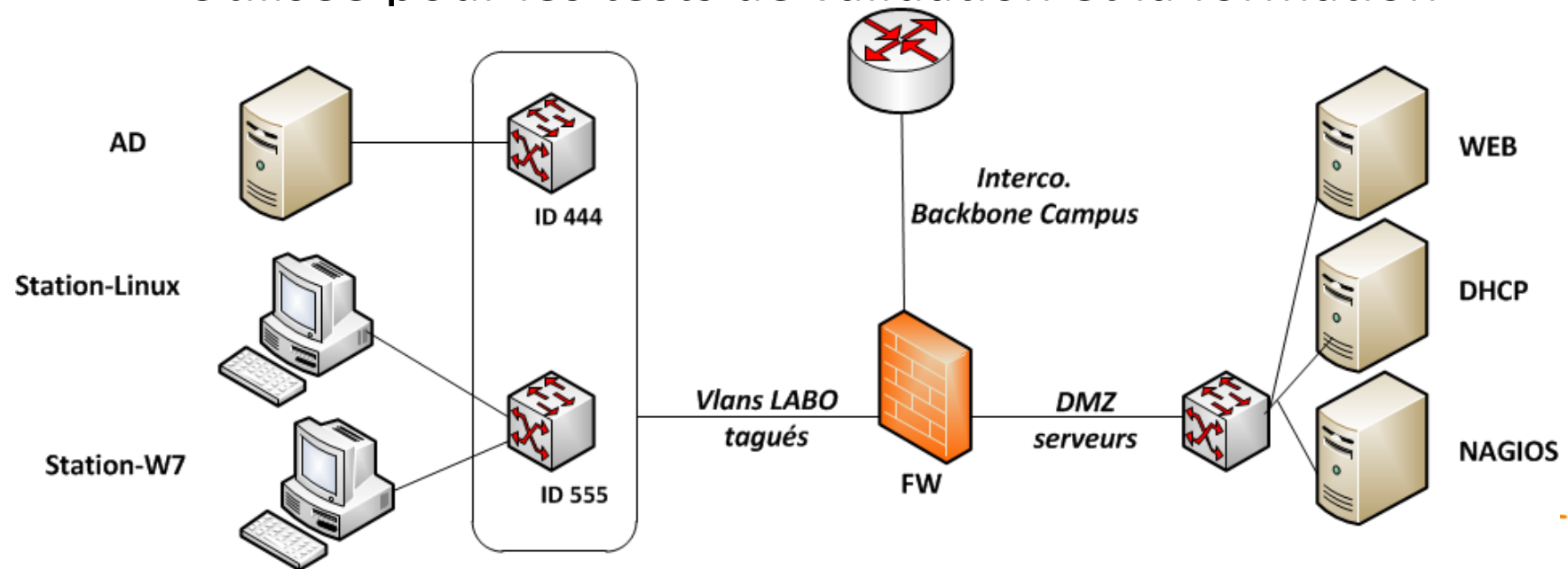
Firewall Builder

Gestion centralisée



La plateforme de test virtualisée

- Un environnement type d'un laboratoire
- Utilisée pour les tests de validation et la formation



Pré-production

- Etape de validation sur un laboratoire
 - Validation des configurations matérielles et logicielles
 - Validation des procédures d'installation
 - Evaluation de la durée de migration
 - Réglages et ajustements



La conduite du changement

- Réunions d'information régulières
- Formation d'une journée et demie assurée par le GT
- Mise en place d'un site collaboratif CORE
- Accompagnement lors des phases de migration
- Suivi de l'exploitation



migration

- Audit
 - Validation des règles utilisées, des services filtrés
 - Vérification de la conformité SSI (filtrage des flux sortants)
- Réécriture des règles
 - Logique de nommage commune
 - Stratégie d'organisation des règles (chaines, branchements)
- Installation et configuration du pare-feu
 - Utilisation d'un master « preseed »
 - Script de post-installation
- Bascule sur le nouveau matériel



La vue d'ensemble de la solution

Serveur EAS

Gestion des pare-feu

Gestion secours

Sauvegardes configurations

Administration des règles de filtrage

Les Pare-feu

Relai DHCP

Syslog

VPN IPsec

Sonde Netflow

Routage Dyn

Scripts NRPE

FILTRAGE iptables/ip6tables

Support

Log

Arch.

Visu.

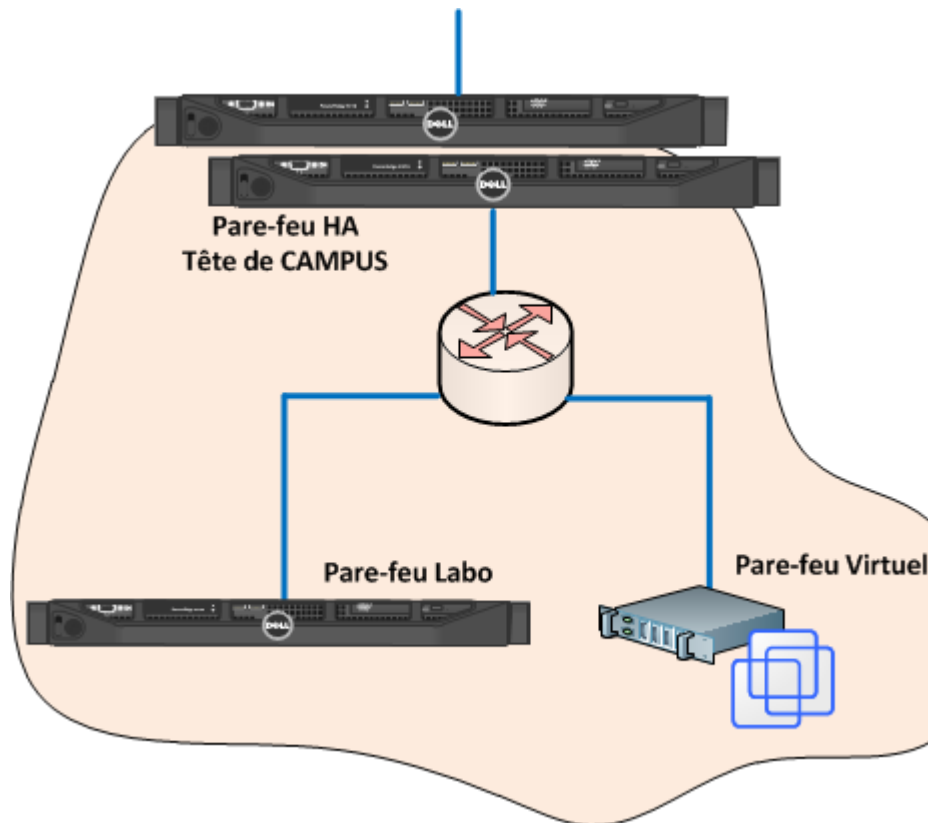
Monitoring réseau

mesures
alertes

Supervision système

mesures
alertes

La partie matérielle



Pare-feu laboratoire:

- 5 * R320 - 4 Go - 6 * 1Gb
- 3 * R210II - 4 Go - 6 * 1Gb
- 2 * pare-feu virtuels

Pare-feu Campus:

- 2 * R420 – 8Go – 6 * 1Gb et 2 * 10Gb

Pare-feu laboratoire

- Distribution Ubuntu 12.04 LTS
 - Netfilter/iptables
 - [+] Quagga (Zebra+ospfd+ospf6d)
 - [+] Ipsec-tools et racoon (VPN-IPsec)
 - [+] Isc-dhcp-relay (relay DHCP)
 - [+] Contrack
 - [+] Nagios NRPE
 - [Ext] la partie sonde de Znets (Netflow)
 - ...



Pare-feu tête de campus

- Distribution Ubuntu 12.04 LTS
 - Idem pare-feu laboratoires
 - [+] KeepAlived (uniquement le module VRRP)
 - [+] Contrackd (synchronisation de la table de sessions)
- Montage haute disponibilité en Actif/Passif



Un point important

- Les temporisations par défaut du *conntrack* de Netfilter (sous Ubuntu) ne sont pas adaptées à un pare-feu.
 - Création d'un script pour modifier les temporisations

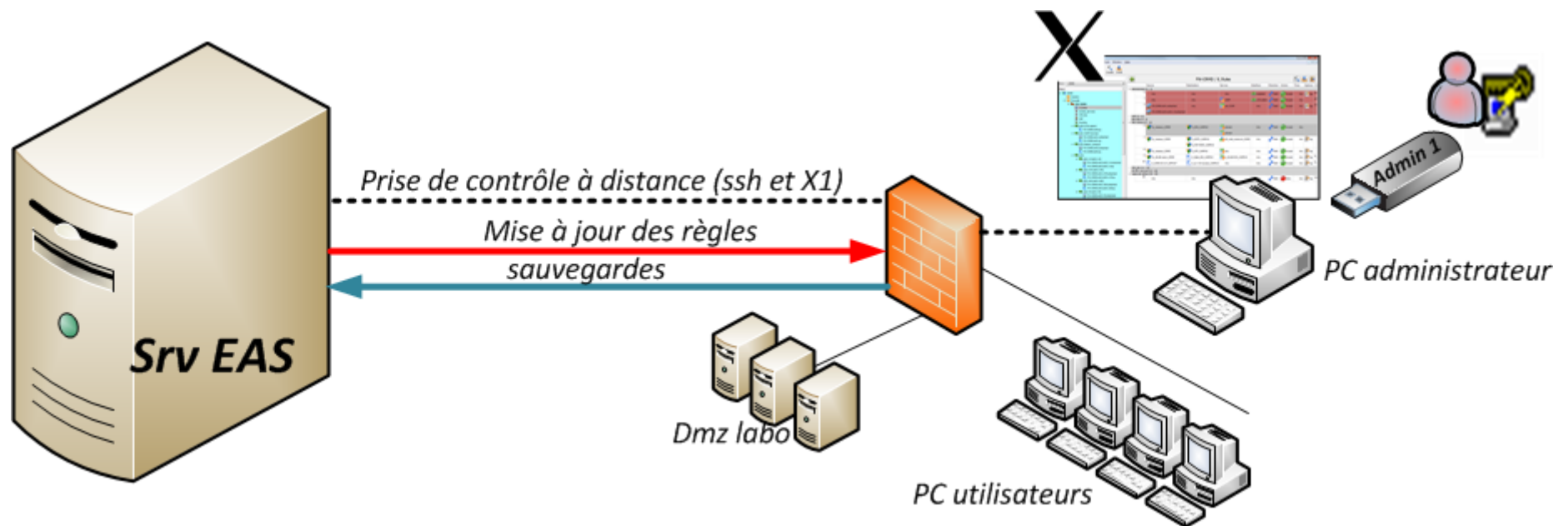
```
net.ipv4.netfilter.ip_conntrack_tcp_timeout_established=86400
net.ipv4.netfilter.ip_conntrack_tcp_timeout_fin_wait=120
net.ipv4.netfilter.ip_conntrack_tcp_timeout_close_wait=3600
...
```

- Utilisation de l'utilitaire *conntrack* pour le débogage

```
sudo conntrack -E -o timestamp | egrep "src=xx\.xx\.xx\.xx "
sudo conntrack -L
```



Le serveur EAS



EAS : *E*dition et *A*dministration des règles de Sécurité

Le serveur EAS

- Centralisation
 - Les 30 dernières configurations sont sauvegardées
- Gestion d'une machine de « secours »
 - Mise à jour automatique
 - Redémarrage par script de la machine de secours avec une config. labo (~10min)
- Centralisation de la gestion des mises à jour
 - Utilisation de la suite Kanif/taktuk (kash, kaput, kaget) [INRIA]
 - Script de mise à jour (retour situation initiale possible):
 - sauvegarde du boot, snapshot LVM, mise à jour de sécurité



Le serveur EAS

- Intérêts :
 - Centralisation
 - des configurations
 - de l'interface d'administration (X11)
 - sauvegardes
 - gestion de la reprise sur incident
 - L'indisponibilité du serveur n'affecte pas le filtrage
- Contrainte :
 - Machine sensible
(authentification par clés SSH, filtrage IP des accès)



Firewall Builder

- Principe:
 - Interface graphique
 - Règles compilées sous forme de script bash
 - Ce script est copié sur le pare-feu pour piloter la configuration des interfaces réseaux et d'iptables
 - Création des règles avec des objets réseaux (adresse, réseaux, services, ...)



Contexte

Conduite du projet

Solution mise en place

Retour d'expérience

Perspectives

Interface graphique

The screenshot displays the Mikrotik WinBox interface for configuring a firewall rule. The main window is titled 'fw-tp1 / 1_table_de_base'. On the left, a tree view shows the project structure under 'User > Firewalls > fw-tp1'. The main area shows a table of firewall rules. The selected rule, '17', is highlighted in red and has the following configuration:

| Source | Destination | Service | Interface | Direction | Action |
|----------------|----------------------------------|------------------|-----------|-----------|--------|
| fw-tp1.eth0:ip | H_CAMPUS_INFRA-FW-SRV-LOG | SG_CAMPUS-syslog | Any | Both | Accept |
| fw-tp1.eth0:ip | H_CAMPUS_INFRA-FW-SRV-monitoring | UDP_LABO-netflow | Any | Both | Accept |
| fw-tp1.eth0:ip | H_CAMPUS_INFRA-Repository | TCP_repository | Any | Both | Accept |
| G_N_CAMPUS | G_N_MON_LABO | ssh | Any | Both | Accept |

Below the table, the configuration for the selected rule is shown in the 'Editor' pane:

- Name: 1_table_de_base
- Rule set: IPv4 and IPv6
- Top ruleset
- Table:
 - mangle table
 - filter+mangle table
- Keywords: No keywords

Interface graphique

The screenshot displays a network configuration interface. On the left, a tree view shows the hierarchy: User > Firewalls > fw-tp1. Under fw-tp1, several tables are listed, with '1 table de base' selected. Other tables include '2_intra-LABO', '3_LABO_CAMPUS', '4_DMZ_9.53.128', '5_ID444_168.53.0', and '6_ID555_9.53.0'. Below the tables are sections for NAT, Routing, and interfaces: eth0 (interco_CAMPUS), eth1 (DMZ), and eth2 (Zone_lab01). Each interface has associated IP addresses and IPv6 addresses. The right pane shows the configuration for the selected table, '1 table de base', with a table of rules:

| Service | Interface | Direction | Action |
|------------------|-----------|-----------|-----------------------|
| SG_CAMPUS-syslog | Any | Both | Accept |
| UDF_LABO-netflow | Any | Both | Accept |
| TCP_repository | Any | Both | Accept |
| ssh | Any | Both | Accept |
| Any | Any | Both | Branch:2_intra-LABO |
| Any | Any | Both | Branch:3_LABO_CAMPUS |
| Any | Any | Both | Branch:4_DMZ_9.53.128 |

Below the table is a comment field with the placeholder text 'Enter comment here' and a 'Keywords...' field with the text 'No keywords'.

Firewall Builder

- Avantages:
 - Outil abouti
 - IHM très réactive (via X11)
 - IHM très proche de l'interface des pare-feu à remplacer
 - Structure et organisation des objets réseaux (groupes, keyword, description)
 - Gestion IPv6 (un objet HOST peut avoir plusieurs IP)
simplification de la gestion « double pile »

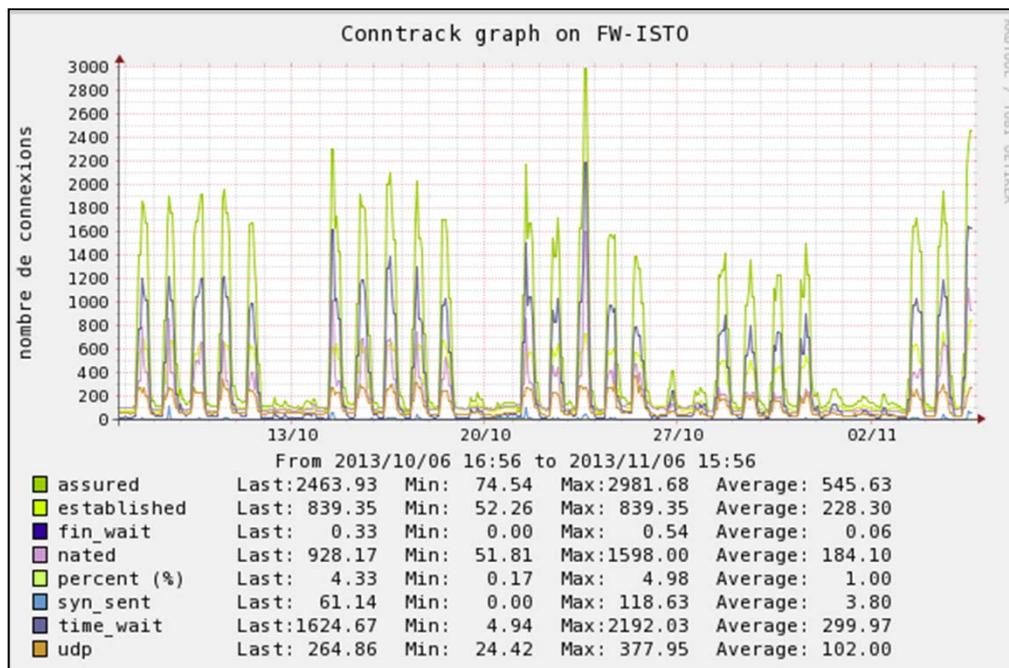


Firewall Builder

- Inconvénients:
 - Ne gère que les règles de filtrage et de NAT (Pas VPN Ipsec, pas relay DHCP)
 - ➔ Mais possibilité d'exécuter des scripts supplémentaires
 - Le gestionnaire de version (RCS) est un peu simpliste
 - Le projet est en veille depuis le mois de juillet 2013 (les concepteurs initiaux sont sur un autre projet)



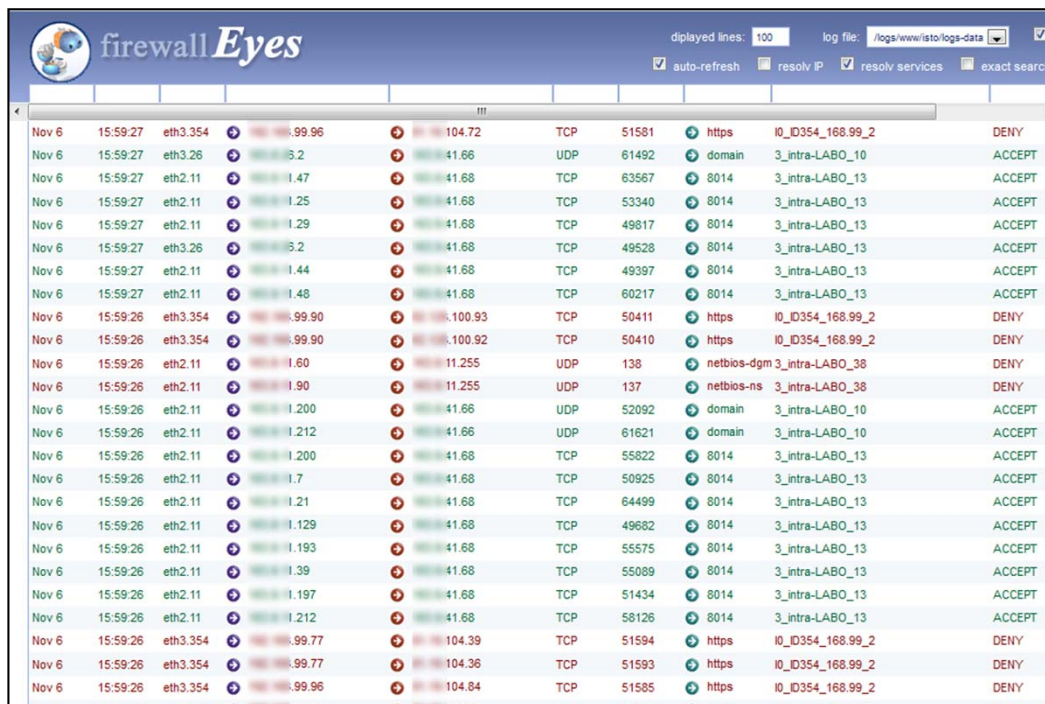
Les outils de support : CENTREON



- Surcouche de Nagios
- Gestion graphique des configurations
- Mesures et Alertes
- Délégation d'administration



Les outils de support : Firewall Eyes

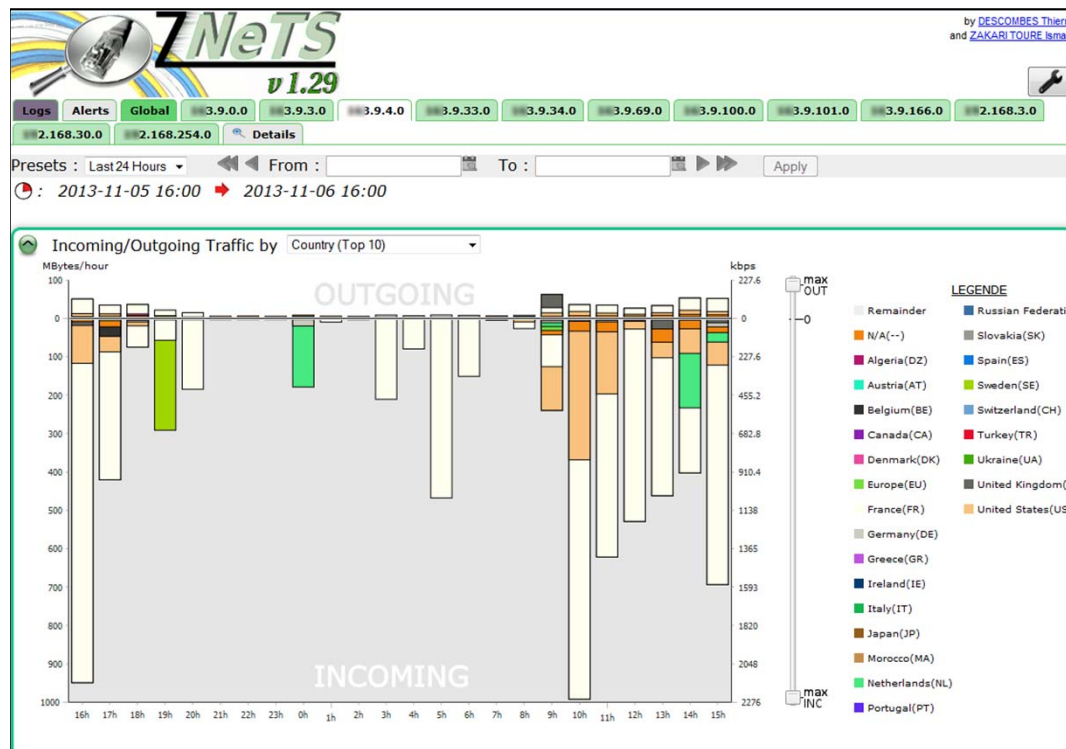


The screenshot shows the Firewall Eyes interface with a log table. The table has columns for date, time, source IP, destination IP, protocol, port, and action. The log entries are as follows:

| Date | Time | Source IP | Destination IP | Protocol | Port | Action |
|-------|----------|-----------|----------------|----------|-------|--------|
| Nov 6 | 15:59:27 | eth3.354 | 104.72 | TCP | 51581 | DENY |
| Nov 6 | 15:59:27 | eth3.26 | 41.66 | UDP | 61492 | ACCEPT |
| Nov 6 | 15:59:27 | eth2.11 | 41.68 | TCP | 63567 | ACCEPT |
| Nov 6 | 15:59:27 | eth2.11 | 41.68 | TCP | 53340 | ACCEPT |
| Nov 6 | 15:59:27 | eth2.11 | 41.68 | TCP | 49817 | ACCEPT |
| Nov 6 | 15:59:27 | eth3.26 | 41.68 | TCP | 49528 | ACCEPT |
| Nov 6 | 15:59:27 | eth2.11 | 41.68 | TCP | 49397 | ACCEPT |
| Nov 6 | 15:59:27 | eth2.11 | 41.68 | TCP | 60217 | ACCEPT |
| Nov 6 | 15:59:26 | eth3.354 | 100.93 | TCP | 50411 | DENY |
| Nov 6 | 15:59:26 | eth3.354 | 100.92 | TCP | 50410 | DENY |
| Nov 6 | 15:59:26 | eth2.11 | 11.255 | UDP | 138 | DENY |
| Nov 6 | 15:59:26 | eth2.11 | 11.255 | UDP | 137 | DENY |
| Nov 6 | 15:59:26 | eth2.11 | 41.66 | UDP | 52092 | ACCEPT |
| Nov 6 | 15:59:26 | eth2.11 | 41.66 | UDP | 61621 | ACCEPT |
| Nov 6 | 15:59:26 | eth2.11 | 41.68 | TCP | 55822 | ACCEPT |
| Nov 6 | 15:59:26 | eth2.11 | 41.68 | TCP | 50925 | ACCEPT |
| Nov 6 | 15:59:26 | eth2.11 | 41.68 | TCP | 64499 | ACCEPT |
| Nov 6 | 15:59:26 | eth2.11 | 41.68 | TCP | 49682 | ACCEPT |
| Nov 6 | 15:59:26 | eth2.11 | 41.68 | TCP | 55575 | ACCEPT |
| Nov 6 | 15:59:26 | eth2.11 | 41.68 | TCP | 55089 | ACCEPT |
| Nov 6 | 15:59:26 | eth2.11 | 41.68 | TCP | 51434 | ACCEPT |
| Nov 6 | 15:59:26 | eth2.11 | 41.68 | TCP | 58126 | ACCEPT |
| Nov 6 | 15:59:26 | eth3.354 | 104.39 | TCP | 51594 | DENY |
| Nov 6 | 15:59:26 | eth3.354 | 104.36 | TCP | 51593 | DENY |
| Nov 6 | 15:59:26 | eth3.354 | 104.84 | TCP | 51585 | DENY |

- Kit PHP (sans base de données)
- Visualisation du fichier de log
- Une instance par laboratoire
- Authentification via LDAP

Les outils de support : ZNeTS



- Outils de statistique réseau
- Une instance par laboratoire
- Archivage des données
- Détection d'anomalies
- Alertes
- Fonctionne avec une sonde cliente (Ipflix netflow 9)



Le bilan ...

- Les 10 pare-feu de laboratoire sont migrés
- Le pare-feu de tête de campus est en production pour IPv6
- La migration a été (quasi) transparente pour les utilisateurs
- Après plusieurs mois d'exploitation bon retour global côté ASR, dans certains cas constatation d'une amélioration des performances pour les utilisateurs



Le bilan ...

- Bon retour du travail d'accompagnement du GT auprès des ASR
- Des étapes sous-évaluées en temps :
 - Phase d'audit (pas liée à la solution retenue)
 - Phase de réécriture des règles
- La phase de migration a été ralentie pour favoriser l'accompagnement des ASR
- La visualisation graphique des logs peut être améliorée



Actions à venir / perspectives

- Mise en place d'un IDPS sur la tête de campus
- Améliorer la gestion et l'analyse des traces
- Déployer IPv6 dans les laboratoires

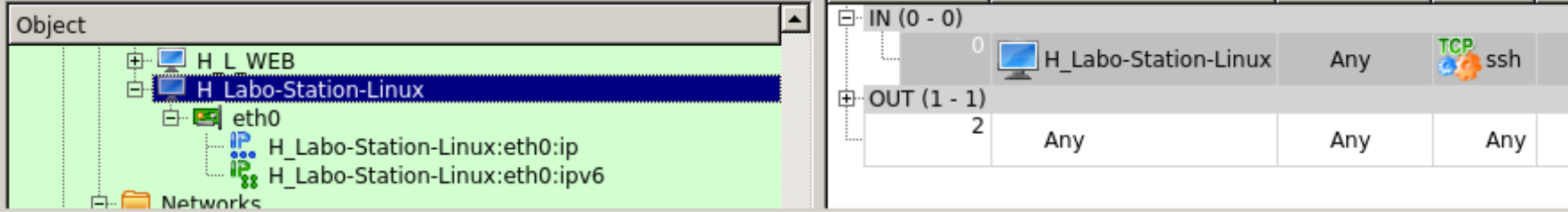


Questions ?



Firewall Builder : Détail règle IPv6

- Un objet HOST est composé de plusieurs IP
- Si détection d'une adresse IPv6 création de règles pour ip6tables



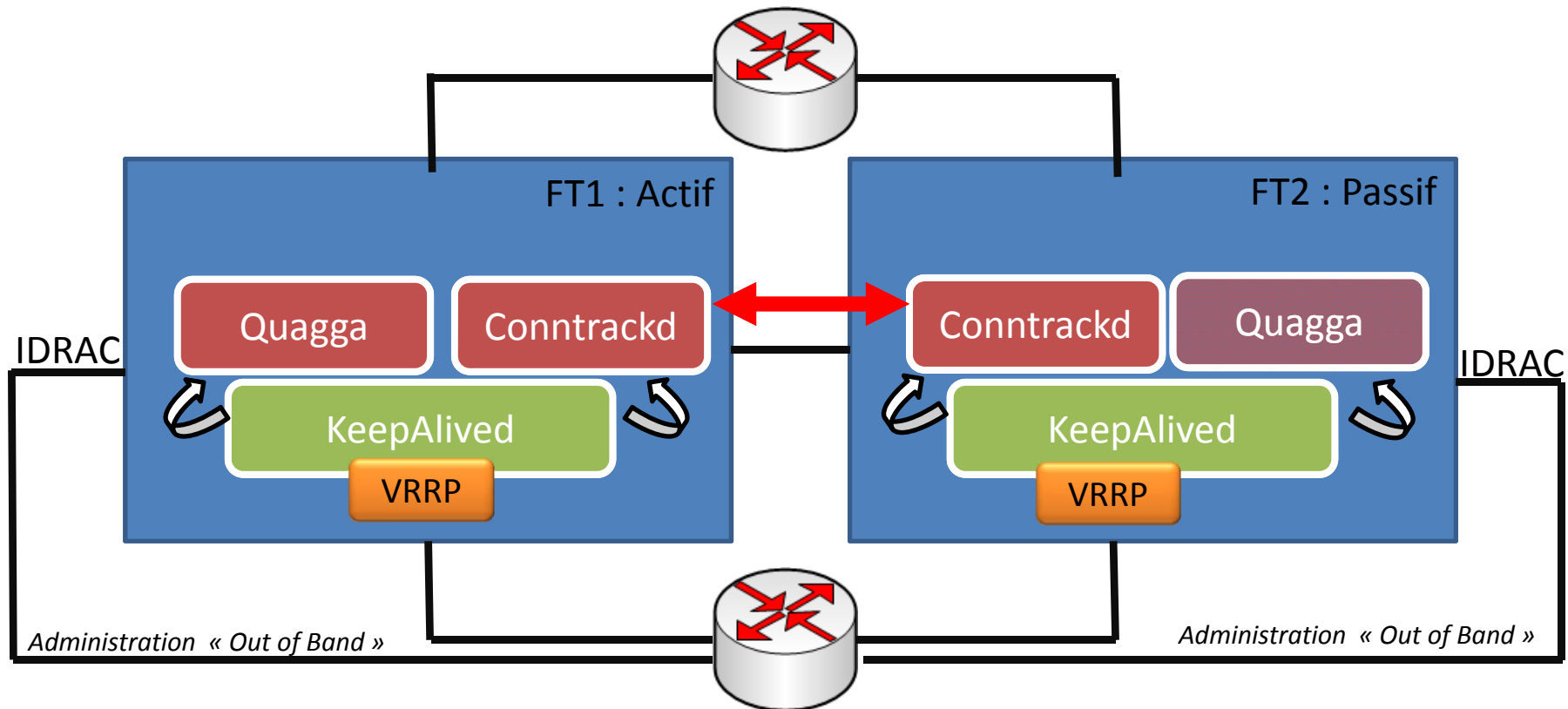
/ User / Firewalls / fw-tp1 / 6_ID555 / rule #0

| Chain | Priority | Source | Destination | Protocol | Service |
|-------------|----------|----------------------|-------------|----------|---------|
| IN (0 - 0) | 0 | H_Labo-Station-Linux | Any | TCP | ssh |
| OUT (1 - 1) | 2 | Any | Any | Any | Any |

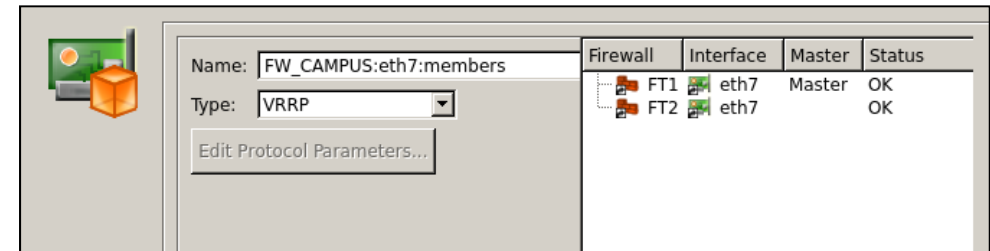
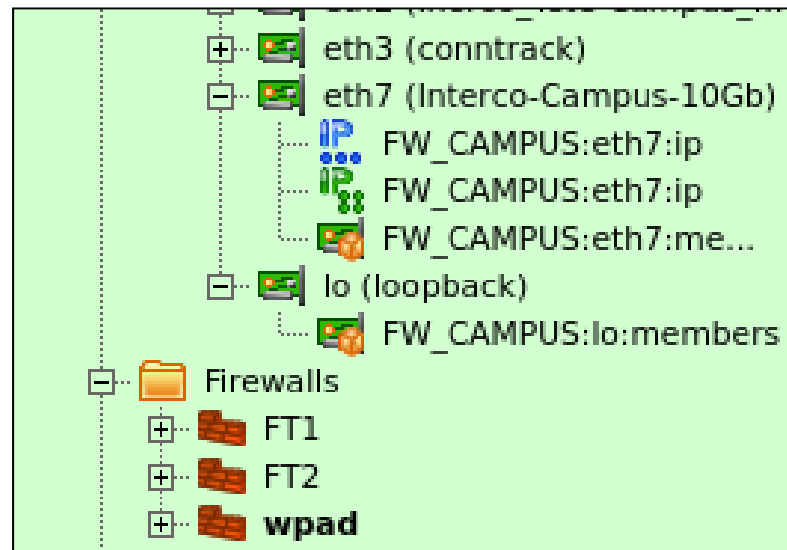
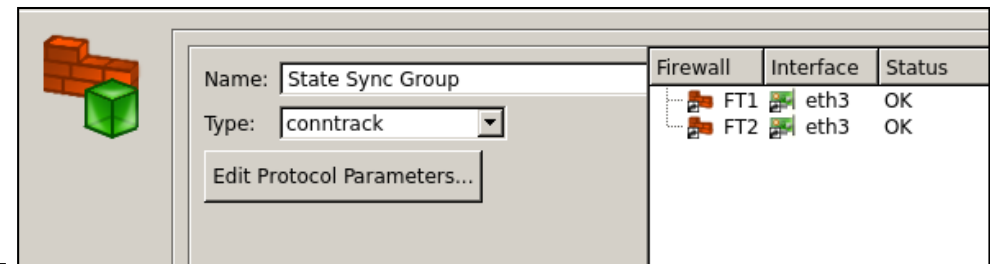
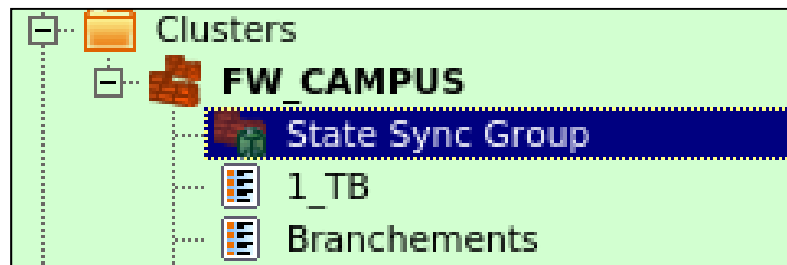
```
fw-tp1 / 6 ID555 / rule 0
$IP6TABLES -N 6_ID555
$IP6TABLES -N 6_ID555_0
$IP6TABLES -A 6_ID555 -p tcp -m tcp -s 2001:660:1::3 --dport 22 -m state --state NEW -j 6_ID555_0
$IP6TABLES -A 6_ID555_0 -j LOG --log-level 6 --log-prefix "RULE ACCEPT 6_ID555_0" --log-tcp-sequence --log-tcp-options --log-ip-options
$IP6TABLES -A 6_ID555_0 -j ACCEPT

$IPTABLES -N 6_ID555
$IPTABLES -N 6_ID555_0
$IPTABLES -A 6_ID555 -p tcp -m tcp -s 169.53.3 --dport 22 -m state --state NEW -j 6_ID555_0
$IPTABLES -A 6_ID555_0 -j LOG --log-level 6 --log-prefix "RULE ACCEPT 6_ID555_0" --log-tcp-sequence --log-tcp-options --log-ip-options
$IPTABLES -A 6_ID555_0 -j ACCEPT
```

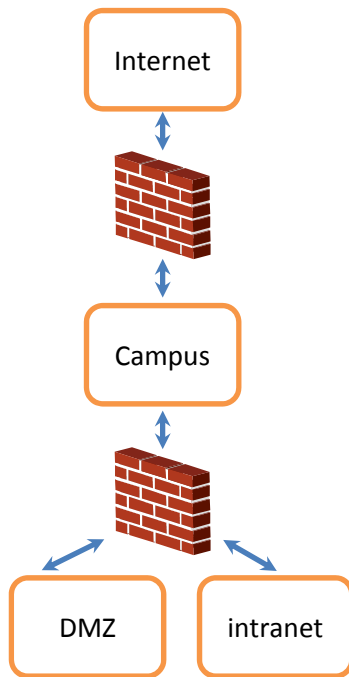
Cluster tête de Campus : principe



Cluster tête de Campus : fwbuilder



Stratégie d'écriture des règles par zones



The screenshot shows the Firewall Builder interface. The main window displays a table of rules for the configuration 'fw-formation / 0_Embranchements'. The table has columns for Source, Destination, Service, Interface, Direction, Action, Time, Options, and Comment. The rules are numbered 0 to 4. Rule 3 is highlighted with an orange box, and an arrow points from it to a text box containing a list of rule categories.

| | Source | Destination | Service | Interface | Direction | Action | Time | Options | Comment |
|---|--------|-------------|---------|-----------|-----------|----------------------|------|---------|-----------------------------------|
| 0 | Any | N_Intranet | Any | Any | Both | Branch:2_vers_Int... | Any | | flux à destination de l'intranet |
| 1 | Any | N_DMZ | Any | Any | Both | Branch:3_vers_DMZ | Any | | flux à destination de la DMZ |
| 2 | Any | N_Campus | Any | Any | Both | Branch:4_vers_Campus | Any | | flux à destination du Campus CNRS |
| 3 | Any | N_Campus | Any | Any | Both | Branch:4_vers_Campus | Any | | flux à destination du Campus CNRS |
| 4 | Any | Any | Any | Any | Both | Deny | Any | log | Normalement, cas impossible |

règles de contrôle des flux de l'intranet vers la DMZ
règles de contrôle des flux internes de la DMZ (VLANs ou réseaux)
règles de contrôle des flux du campus vers la DMZ
règles de contrôle des flux de l'internet vers la DMZ