

LINUX ET LA SECURITE, PROXY ET FIREWALL

METHODE PEDAGOGIQUE

Pédagogie interactive-
Alternance d'apports
théoriques et pratiques

PRE-REQUIS

Avoir suivi la formation
«Administration de base
d'un poste client» ou
connaissances équivalentes.
Cette formation requiert
donc la connaissance et la
pratique de l'administration
d'un serveur Linux et du
protocole TCP/IP

DUREE DU STAGE

2 jours

LIEU

**Centre de Ressources
Informatiques**
199 route de Clisson - CS 13511
44235 St Sébastien s/L Cedex

ou

Sur SITE

PUBLIC

Tout administrateur amené
à installer et à configurer
des applications Internet
sous Linux

PROCHAINES SESSIONS AU CRI

Les 20-21/06/2011

**Stage personnalisé
ou sur site :**

Nous consulter

OBJECTIFS

SAVOIR ADMINISTRER, INSTALLER ET GERER LA SECURITE DE BASE INTERNET

PROGRAMME DU STAGE

NOTIONS DE SECURITE

- Pourquoi se soucier de la sécurité ?
- Sécurisation d'un réseau
- Le chiffrement
- Tout service est un danger potentiel
- La surveillance des connexions
- Redirection et réécriture dynamique d'URLs
- Le moyen de s'informer
- Mettre à jour les applications

LE MANDATAIRE/CACHE SQUID

- Généralités
- Fonctionnement de Squid
- Les besoins matériels
- Fichiers de configuration
- Configuration du cache
- Le contrôle des accès
- La gestion des journaux

FIREWALL

- Les outils disponibles
- Comment partitionner un pare-feu
- Définir une politique de sécurité
- Les trois phases de tri possible
- Manipuler les règles de filtrage
- Les critères de la couche internet
- Les critères de la couche transport
- La gestion des fragments
- Tester et valider la configuration
- Les filtres personnalisés
- La traduction d'adresses
- La redirection de port
- Les serveurs mandataires transparents