Mise en œuvre de routeurs

Gatien GASPARD - Plan-Net S.A

Licence Professionnelle ASRALL, promotion 2009

29 juin 2009

Table des matières

Le projet

Dans le cadre de mon stage chez Plan-Net S.A, j'ai été amené à effectuer un certain nombre de tâches parmi lesquels :

- Recherche et expérimentation sur la QoS
- Installation et configuration de routeurs chez des clients
- Création d'un script pour automatiser l'installation des routeurs
- Migration des parefeux de la société
- Recherche sur la détection d'intrusion

La qualité de service

- Qu'est-ce que c'est ?
  - La gestion de bande passante
  - Du matériel de qualité
  - De la redondance
- Quel interêt ?
  - Garantir un service minimum pour le client
- Exemple : 4 clients se partagent une connexion 8 Mbit.

La QoS, quels outils

- Webmin-Htb
- MasterShaper
- WonderShaper
- TC et IPtables
- FWBuilder
- QtMonitor

Aperçu de Webmin-Htb

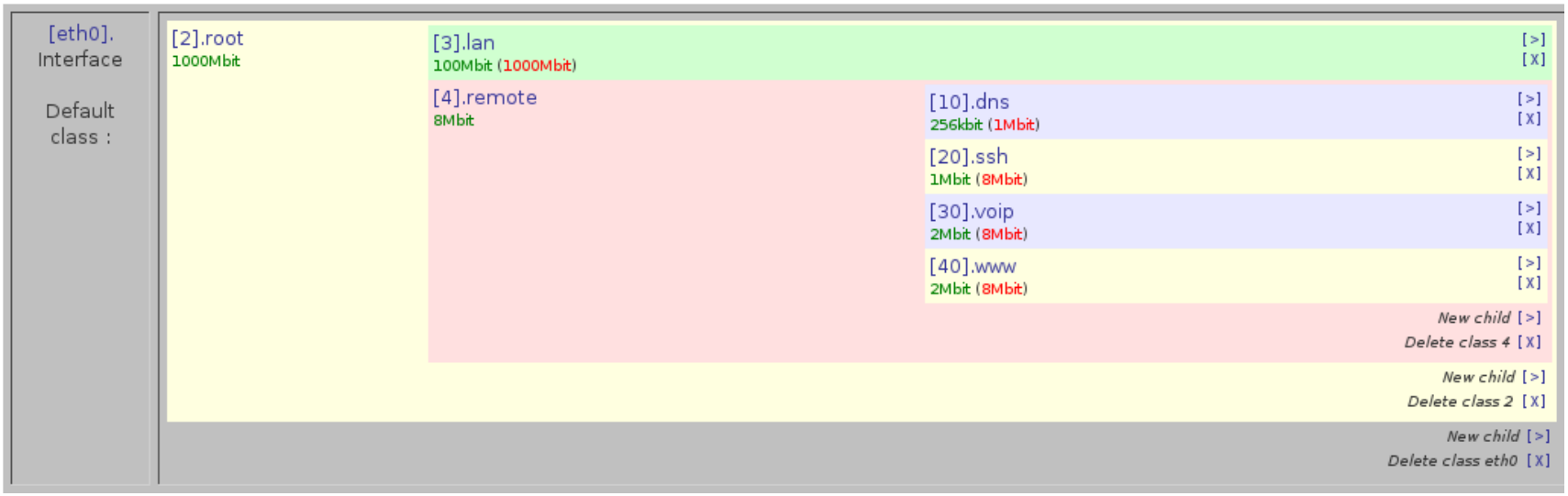

FIG.: Aperçu de Webmin-Htb : (limitation de bande passante)

Aperçu de QtMonitor

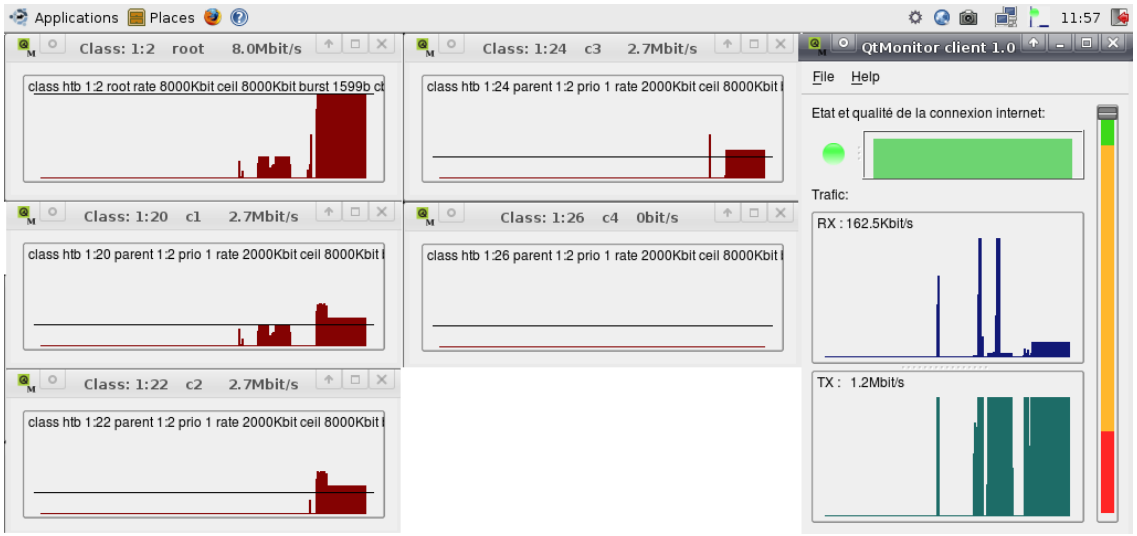

FIG.: Aperçu de QtMonitor : Visualisation de la bande passante par classe

FWBuilder, un outil très utile

Avantages :

- Gestion simplifiée et centralisée de parefeux
- Gestion des règles de NAT et de routage en plus du filtrage
- Marquage de paquet (pour QoS)
- Outil graphique

Inconvénients :

- Manque de fonctionnalités au niveau de l'interface (ergonomie)
- Système de gestion des objets par identifiants
- Impossible de créer des objets directement en éditant le fichier

Aperçu de FWBuilder

loopback-net	loopback-net	Any	loopback	Both	Accept	Any
Intranets Plan-Net Plan-Net VPN	Any	Services INT	inside	Inbound	Accept	Any
Intranets Plan-Net	manage	Any	manage	Both	Accept	Any
Plan-Net trusted hosts	outside	Any	outside	Inbound	Accept	Any
Any	outside	Services EXT OpenVPN	outside	Inbound	Accept	Any
outside	Any	Any	outside	Outbound	Accept	Any
Intranets Plan-Net Plan-Net VPN	Intranets Plan-Net Plan-Net VPN	Any	All	Both	Accept	Any
Postini servers range	outside	SMTP Mail	outside	Inbound	Accept	Any
Stix-Cerbere LAN	Intranets Plan-Net Plan-Net VPN	Any	outside	Both	Accept	Any
Any	rfc1918-nets broadcast	Any	outside	Both	Deny	Any
rfc1918-nets broadcast	Any	Any	outside	Both	Deny	Any
Interfaces VPN Plan-Net distantes	Plan-Net LAN Rumelange	Any	All	Inbound	Accept	Any
Office LAN Belval Projo Ciné LAN Belval	Plan-Net LAN Rumelange	Any	All	Inbound	Accept	Any

FIG.: Aperçu de FWBuilder : Règles

Automatiser l'installation des routeurs

Installation d'un routeur avant ce script :

- Complexe (nombreuses étapes)
- Relativement long

Installation à l'aide du script crée :

- Copie de l'image depuis le serveur NFS
- Personnalisation du système
- Mise à niveau du système
- Système stable et opérationnel

La migration des parefeux

À l'origine :

- Règles de parefeux : /etc/SuseFirewall2
- Règles de NAT : /etc/SuseFirewall2 et /etc/rinetd
- Table de routage : chargée depuis un script au démarrage
- Chacun de ces éléments se retrouve sur chaque routeurs

Après migration :

- Règles dans en un unique fichier objet de FWBuilder
- Gestion centralisée des parefeux depuis ce fichier
- Fichier complet disponible sur chacun des parefeux installés

Ajouter une seconde connexion Internet à Belval

- Ajout d'une connexion PPPOE[1]
- Mise à jour du serveur à Londres et des monolythes Modification de /etc/ssh/sshd_config :
  - TCPKeepAlive yes
  - ClientAliveInterval 15
- Temps d'inaccessibilité des monolythes : 15 secondes

[1] PPPOE : point to point protocole over Ethernet

La mise en place de tunnels VPN

- Tunnel VPN avec SSH :
  - Ajouter *PermitTunnel point-to-point* et *PermitRootLogin yes* au fichier sshd_config sur le serveur.
  - sudo ssh -w 1 :0 root@example ifconfig tun0 192.168.0.1 192.168.0.2
  - ifconfig tun1 192.168.0.2 192.168.0.1
- Tunnel VPN avec OpenVPN :
  - Un fichier de config dans /etc/openvpn
  - Une clé partagée pour sécuriser la connexion

La détection d'intrusion

- Snort + BASE
- Permet d'alerter qui de droit en cas d'intrusion
- Nécessite énormément de ressources
- Impossible de l'utiliser depuis les routeurs de la société

Conclusion

- Stage très intéressant
- La QoS peut être utile pour des structures peu importantes
- La détection d'intrusion nécessite beaucoup de ressources
- La configuration de parefeux centralisée à de nombreux avantages

Des questions ? ? ?

- À vos questions ! ! !

Remerciements

- La société Plan-Net
- L'IUT Nancy Charlemagne
- Vous qui avez pris la peine de m'écouter