Expérience de mise en œuvre d'un garde-barrière sous Linux:LABWALL

Serge Bordères
Centre d'Etudes Nucléaire de Bordeaux-Gradignan
Domaine du Haut-Vignaux BP 120 33175 Gradignan
Borderes AT cenbg.in2p3.fr
Date: 13/10/2003

1 Qu'est-ce-que LabWall ?

Labwall est un projet de développement d'un routeur/garde-barrière sous Linux et Netfilter. Ce projet a été lancé en Mai 2001 au centre d'Etudes Nucléaire de Bordeaux-Gradignan (CENBG). La motivation en était la volonté de segmenter le réseau interne en plusieurs sous-réseaux. Ceci d'une part pour des raisons fonctionnelles (le CENBG abrite dans ses locaux un autre laboratoire) et d'autre part à des fins de sécurité puisqu'il devenait possible de créer une zone démilitarisée (DMZ) -et même plusieurs- ou encore un réseau visiteur.
Labwall fut imaginé avec trois principales spécifications qui devaient assurer la faisabilité du projet.
Tout d'abord Labwall devait être capable de router des réseaux basés sur des vlans afin de pouvoir bénéficier des capacités des commutateurs déjà installés (Cisco 2924). Cette option permet de router l'ensemble des sous-réseaux internes avec une seule carte Ethernet.

La disponibilité était le deuxième critère important. En effet, une telle fonction est assurée par une machine placée au milieu du réseau et donc une panne doit être résolue dans un délai très court. Ce fut la principale raison qui écarta une solution commerciale, un contrat de maintenance ne permettant pas des délais suffisamment courts, et l'achat de deux machines spécialisées étant proscrit. C'est pour ça que la solution Labwall est basée sur une machine de type PC sous Linux, facilement remplaçable.
Mais ce n'était pas suffisant. Le système devait être booté en mémoire depuis un CD-ROM. Donc pas de disque qui tombe en panne et une capacité de reprise très rapide sur une autre machine (pas de ré-installation, il suffit de la booter sur le CD). Comme il n'existait pas de méthode satisfaisante, il fut mis au point une méthode qui est devenue un projet à part entière : CDNUX. Il ne s'agit pas d'une distribution spéciale de Linux mais d'une méthode consistant à générer un système Linux sur un CD à partir de celui déjà installé sur un poste. Ceci présente donc l'intérêt d'utiliser « sa » distribution Linux, celle qu'on fréquente tous les jours et donc sans faire appel à une distribution très spécifique qu'il faut suivre, mettre à jour etc, etc. L'autre avantage c'est que CDNUX n'est pas une méthode dédiée à une application de garde-barrière. Tout ce qu'on peut installer sur son poste peut être mis sur le CD. En fait Labwall est une application embarquée de CDNUX (bien qu'il soit parfaitement capable de fonctionner sur un système " classique ", c'est-à-dire avec un disque).

La troisième spécification était de simplifier au maximum l'écriture des règles de la politique de filtrage. En effet, écrire directement des commandes Iptables (l'outil de configuration de netfilter) devient vite illisible et assez délicat.
Labwall met en œuvre des scripts Bash, appelés macros, qui réalisent chacun une fonction de filtrage particulière avec la syntaxe la plus simple possible. Labwall introduit également la notion de « filtrage structuré » pour clarifier la politique de filtrage mais aussi pour optimiser les performances.
Ces macros sont très simples, uniquement écrites en Bash, il n'y a aucun programme à compiler, aucune librairie etc..

2 Configuration du réseau du garde-barrière.

Labwall dispose d'un premier fichier de configuration permettant de paramétrer facilement son réseau, surtout quand on commence à avoir un grand nombre de sous-réseaux. Il permet de voir toute sa configuration d'un seul coup d'œil.
Il est possible de configurer des architectures simples (garde-barrière transparent) comme des plus élaborées (plusieurs sous-réseaux sur vlan).
On peut également définir simplement des règles de translation d'adresses (masquerade, snat, dnat, static). Depuis la version 2.4.14, le noyau Linux contient en standard le support des vlans 802.1q [4]. La carte Ethernet qui est tournée vers l'intérieur doit être connectée sur un port d'un switch configuré en « TRUNK ».
Dans le cas d'une configuration comme garde-barrière transparent, il se comporte comme un pont. Pour cela il est nécessaire d'appliquer le patch bridge-nf (ebtables [3]) afin de pouvoir bénéficier de toutes les possibilités de Netfilter. (Ce patch est intégré dans les noyaux supérieurs à 2.4.x). Il est également possible de combiner pont et routage.
Des exemples de configurations peuvent être trouvés sur le site web de Labwall.[1].

3 Les fonctions de filtrage

Toutes les règles de filtrage sont écrites dans un deuxième fichier de configuration sous forme d'appel à des macros. Chacune réalise une fonction de filtrage particulière en exécutant des commandes Iptables/Netfilter [2]. Par exemple si on veut autoriser une adresse ip1 à ouvrir une communication Telnet vers une adresse ip2 on écrira simplement : TELNET ip1 ip2 .
Si au contraire on veut l'interdire on écrira : NOTELNET ip1 ip2.
Ce principe de macros permet de dépouiller la politique de filtrage de tout aspect de syntaxe et donne beaucoup de lisibilité à l'ensemble et facilite grandement la gestion quotidienne.
Une autre particularité importante a été baptisée "filtrage structuré " ou encore "filtrage programmé ". Il s'agit de concevoir le parcours d'un paquet à travers les règles de filtrage comme on conçoit un programme. C'est-à-dire un programme principal qui appel des sous-programmes. Chaque paquet traité va " exécuter " ce programme. Avec cette technique non seulement la politique de filtrage devient très structurée mais en plus on optimise considérablement les performances. En effet les paquets vont parcourir uniquement des règles qui les concernent.
Ces "sous-programmes ", appelés "zones", peuvent représenter des sous-réseaux, des listes de machines, des protocoles ou des devices (eth). Là aussi on utilise uniquement des fonctions standards de Iptables/Netfilter.
Le principe consiste à écrire par exemple (toujours à l'aide des macros simples) :
Pour chaque paquet
Si le paquet a pour destination une adresse du sous-réseau de la DMZ alors balayer les règles de la zone DMZ.
Si le paquet a pour destination une adresse du sous-réseau VISITEURS alors balayer les règles de la zone VISITEURS.
Des exemples complets de configurations peuvent être trouvés sur le site web de Labwall [1].

4 Mode "apprentissage"

Les macros décrites ci-dessus exécutent des commandes du type « ifconfig », « route »… pour la configuration réseau et des commandes Iptables pour les règles de filtrage. Lorsqu'on enclenche le mode apprentissage (LEARN) au lieu d'être exécutées les commandes sont écrites dans un fichier. Ce fichier est un script Bash qui contient tout le nécessaire pour configurer un garde-barrière. Il peut donc être installé et exécuté sur une autre machine qui n'a pas besoin des programmes de Labwall. Cela permet de gérer à partir d'un seul poste les configurations de plusieurs routeurs/gardes-barrière.

5 Bilan

Labwall est en exploitation au CENBG depuis le début 2002 sans aucun dysfonctionnement et sans provoquer de chute de performances sensibles. Dans le réseau du CENBG qui compte environ 300 adresses IP, 150 utilisateurs, sa consommation CPU, en exploitation, dépasse rarement 14% pour un processeur 1Ghz. Dans le cas d'utilisation de CDNUX, l'utilisation de la mémoire est de l'ordre de 80Mo, y compris le système de fichier de Linux.
Labwall+CDNUX ont atteint leurs objectifs initiaux. Ils ont permis d'anticiper des besoins de sécurité interne qui se présentent aujourd'hui et qui peuvent désormais être satisfaits très facilement et rapidement (nomades personnels, visiteurs, sous-réseaux protégés…). Et ce sans développement sophistiqué et en se basant sur la culture Linux déjà existante.
Les outils ainsi créés et l'expérience qui en découle ont permis un prolongement dans des "produits dérivés" comme un DNS booté sur CD ou encore le projet Mobilnet. Il s'agit d'un réseau mobile destiné aux chercheurs qui partent avec du matériel sur des expériences sur d'autres sites. Cela leur permet d'être opérationnel sur le réseau d'accueil en quelques minutes au lieu de parfois une journée auparavant.
D'un point de vue général, cette expérience a montré qu'un garde-barrière peut être bien accepté et qu'en plus le travail investi peut se prolonger pour apporter de nouveaux outils aux chercheurs.

Références :
[1] LABWALL, CDNUX, MOBILNET : http://www.cenbg.in2p3.fr/network.html
[2] Netfilter : http://www.netfilter.org
[3] Bridge-nf , ebtables : http://sourceforge.net/projects/ebtables
http://users.pandora.be/bart.de.schuymer/ebtables/br_fw_ia/br_fw_ia.html
[4] Support vlan 802.1q : http://www.candelatech.com/~greear/vlan.html