m0n0wall

Présentation pour le groupe SUR
(Sécurité Unix et Réseaux)
de l'OSSIR

Maxime Brémond et Guy Widloecher

m0n0wall

Un firewall en logiciel libre
Retour d'expérience

Un peu de vocabulaire

- m0n0wall s'écrit avec des chiffres 0 (zéros) non des lettres o ou O
- Mais beaucoup de gens se trompent (Google s'en sort bien : en tapant avec des o, il rend le site classé 1er)
- Le site : http://m0n0.ch/wall/

Notre expérience

- Le projet : mettre en oeuvre rapidement un firewall (un vrai) pour un petit LAN dédié raccordé à Internet chez VINCI
- En faisant attention au coût, hardware minimal
- Pas d'impératifs particuliers de performance et de redondance
- Nous avons pensé à m0n0wall

Notre expérience

- Nous en avons profité pour valider que m0n0wall puisse s'intégrer dans un réseau d'entreprise déjà existant :
  - plan d'adressage complexe
  - VPN IPSEC
  - administrable à distance
  - logging, surveillance, remontée d'alarme
  - environnement très hétérogène

Présentation de m0n0wall

- Un firewall digne du marché sur un PC (tout hardware supporté par FreeBSD4 pour i386 – tourne sur Nokia Série IP!!!)
- En logiciels libres
- Basé sur du FreeBSD4 et ipfilter/ipnat
- Administrable via browser en PHP qui masque tout le système sous-jacent
- Configuration en fichier XML

Présentation de m0n0wall

- Un site web agréable (bon point!)
- De nombreux articles et échanges sur le web au sujet de m0n0wall
- Peu de critiques et bugs
- Bonne documentation (presque finie)

Le coupable c'est lui : Manuel Kasper

Un développement récent

- 1ère release beta en février 2003
- Version 1 en février 2004
- Dernière version 1.21 le 1er janvier 2006
- Un groupe d'environ 30 personnes
- Mailing-list très active

Un système très compact

- Il fait moins de 6M
- Bootable sur Cdrom, Compact-Flash ou disque
- Configuration sur Cdrom, disquette, Compact-Flash ou disque
- Possibilité de tourner avec un Cdrom uniquement (OS et configuration en read-only)
- Tourne sur 64M minimum

Les composants

- required FreeBSD components (kernel, user programs)
- ipfilter
- PHP (CGI version) et mini_httpd
- MPD
- ISC DHCP server
- ez-ipupdate (for DynDNS updates)
- Dnsmasq (for the caching DNS forwarder)
- racoon (for IPsec IKE)
- UCD-SNMP, choparp et BPALogin

Les fonctions

- Principales fonctions :
  - web interface (supports SSL)
  - serial console interface for recovery
  - wireless support
  - captive portal
  - 802.1Q VLAN support
  - stateful packet filtering
  - NAT/PAT
  - DHCP client, PPPoE, PPTP and BigPond support on the WAN interface

Les fonctions (suite)

- IPsec VPN tunnels
- PPTP VPN
- static routes
- DHCP server and relay
- caching DNS forwarder
- DynDNS client and RFC 2136 DNS updater
- SNMP agent
- traffic shaper
- SVG-based traffic grapher
- firmware upgrade through the web browser
- Wake on LAN client

Performances

- Soekris 45xx (133 MHz) 17 Mbits/s
- Soekris 48xx (266 MHz) 40 Mbits/s
- WRAP PC Engines (266 MHz) 40 Mbits/s
- PC/Pentium (bonnes cartes Ethernet) 40 Mbits/s
- PC/Pentium III (bonnes cartes Eth) 100 Mbits/s
- PC/P4 2.8 GHz (bonnes cartes Eth) 1000 Mbits/s
- Bonnes cartes Ethernet : chipset Intel par exemple
- Mauvaises cartes Ethernet : chipset Realtek par exemple

Ce que nous avons aimé

- Epoustouflant !
- Facilité de mise en oeuvre, de configuration, d'administration (très facile et intuitif)
- Intégration facile dans un grand réseau avec toutes ses contraintes architecturales
- Pas de licence à gérer (ceux qui utilisent Firewall-1 comprendront!)

Ce que nous avons aimé

- Translation sur les adresses source et destination simultanément (impossible avec FW-1 par exemple)

Ce que nous avons moins aimé

- Limitation du NAT sur l'interface LAN
- Pas de haute disponibilité (non nécessaire pour notre projet mais indispensable pour le futur)
- Une configuration des tunnels IPSEC un peu lourde
- Pas de règle de filtrage sur les tunnels IPSEC

Ce que nous avons moins aimé

- Règles interface par interface
- Objets (alias) très pauvres (pas de groupes, pas de ports TCP ou UDP) donc peu pratique pour gérer une configuration complexe

Ce qui est souvent reproché par les autres

- Pas de load balancing ou de redondance
- Pas d'outils (nmap, tcpdump, ethereal...)
- Pas de fonctions évoluées (anti-virus, anti-spam, IPS, proxy, filtrage d'URL...)
- Manuel Kasper s'oppose à la plupart des demandes pour garder un « vrai » firewall compact.

Un fork du projet m0n0wall : pfSense

- Le site http://www.pfsense.com/
- Basé sur Packet Filter
- Ajout de nombreuses fonctionnalités par rapport à m0n0wall
- Malheureusement pas utilisable pour l'instant (trop de bugs !)

Les prochains développements

- plus de possibilités en wireless
- vérification du fichier XML
- gestion des certificats
- levée de limitation sur interface LAN
- quick setup wizard
- notion de groupes d'objets
- NAT sur protocole IP
- blacklistage sur détection de scan
- statistiques par IP
- support adresse secondaire sur WAN

Les prochains développements (suite)

- possibilité de load balancing
- règles basées sur heure et date
- lien de backup dialup
- possibilité de GUI en read-only
- haute disponibilité (VRRP ou CARP)

Une capture d'écran

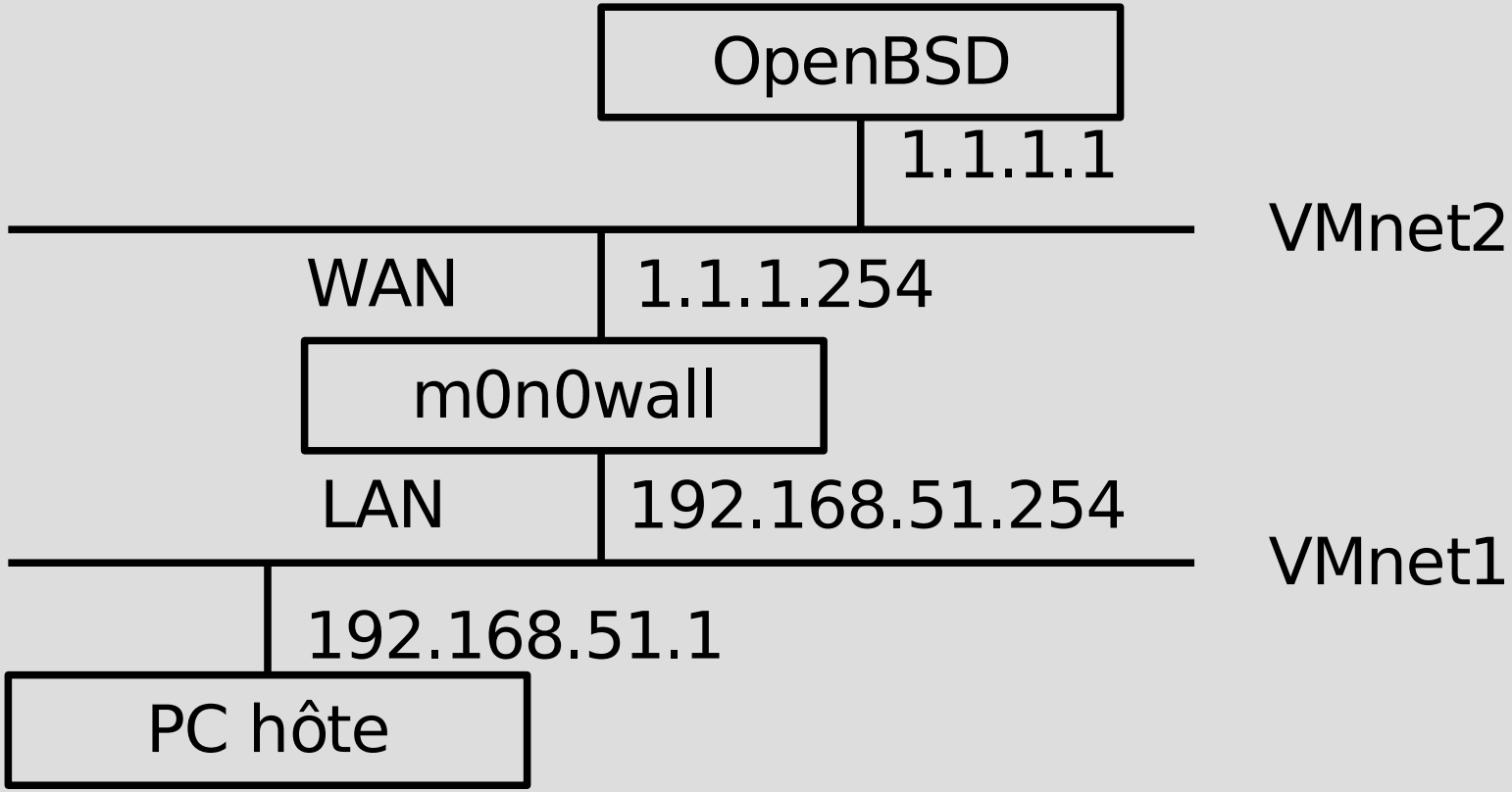
Démonstration

- Sous Vmware
- Création d'une machine m0n0wall
- Avec 2 interfaces
- Une (LAN) vers le PC hôte via le LAN virtuel VMware prévu à cet effet
- Une (WAN) vers l'extérieur, un LAN virtuel VMware sur lequel se trouve une machine OpenBSD

Démonstration

- Nous allons faire la configuration de base du m0n0wall
- Créer quelques règles pour l'administrer
- Créer une règle pour permettre le passage d'un flux TCP vers le WAN
- Voir les translations d'adresses
- Visualiser la configuration XML

Démonstration



Nous contacter

- mbremond < at > vinci.com
- gwidloecher < at > vinci.com

Remerciements

- A Monsieur Ph.Bavay, Directeur Informatique de Vinci, de nous avoir permis d'en parler
- A vous, auditoire du groupe SUR
- A tous les développeurs de logiciels libres impliqués de près ou de loin dans le projet m0n0wall et particulièrement à Manuel Kasper