Outils de sécurité réseau avec OpenBSD et PF

Matthieu Herrb

LAAS-CNRS

Université de Toulouse

JRES 2011

Agenda

Agenda

Introduction

LAAS-CNRS : laboratoire de 650 personnes.

- Besoin de solutions de sécurité :
  - filtrage de paquets
  - accueil des visiteurs
- Intéressés par logiciels libres depuis longtemps

$\Rightarrow$ Choix d'OpenBSD + PF

Agenda

OpenBSD...

- Système d'exploitation Unix-like multi-plateformes
- Dérivé de BSD 4.4
- Noyau + utilitaires + documentation maintenus ensemble
- Applications tierces disponibles via ports
- Une version tous les 6 mois
- Architectures matérielles: i386, amd64, alpha, sparc, sparc64, macppc, arm,...

Qu'est-ce que PF ?

- Filtre de Paquets réseau niveau 3
- Intervient sur le trafic entrant ou sortant d'une interface
- Permet de :
  - bloquer/autoriser le paquet à continuer son chemin
  - placer un label sur le paquet
  - modifier le paquet (NAT, ...)
  - re-diriger le paquet vers une autre destination

Filtrage à état (stateful)

- Les protocoles réseau sont gérés par des automates (exemple: TCP)
- PF suit l'état de l'automate pour les protocoles connus
- Cela permet de :
  - détecter les paquets qui violent le protocole
  - limiter la complexité des règles de filtrage en laissant passer automatiquement les paquets valides du protocole.
  - contrôler les ressources utilisées par le filtre

Règles de PF

- Stockées dans `/etc/pf.conf`
- S'appliquent au niveau 3 (IP, ICMP, TCP, UDP, ...)
- Lues dans l'ordre où elles apparaissent
- La **dernière** règle qui matche un paquet s'applique.
  (Attention : différent de Cisco / Linux ...)
- Si une règle modifie un paquet, le paquet modifié est utilisé en entrée des règles suivantes.
- Les tables permettent de traiter des listes dynamiques d'adresses IP

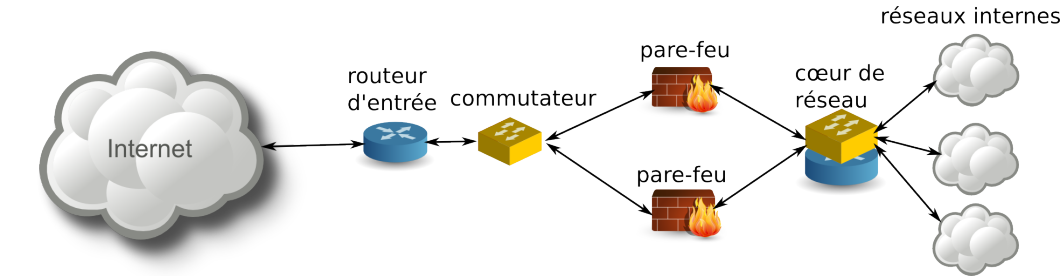
Agenda

Besoin

- Filtrage de paquets avec état
- Compatible routage IPv6 + multicast
- Continuité de service
- Possibilité de retour arrière en cas de problème

$\Rightarrow$ choix d'une solution en mode bridge.

Mode bridge - Redondance



Deux approches possibles :

- agrégation de liens
- arbre de recouvrement

Choix : arbre de recouvrement (RSTP).

Quelques exemples de filtrage

- Accès aux services connus seulement sur serveurs désignés
- Limitation du nombre de connexions vers serveurs SSH
- Isolation complète de certaines machines internes
- Limitation des accès sortants de machines considérées comme infectées
- Blocage de machines extérieures identifiées comme malveillantes

Administration

Modifications des règles : édition du fichier `pf.conf` sur le pare-feu maître

puis script qui :

- valide la syntaxe (`pfctl -n`)
- copie le fichier vers le second pare-feu
- charge les nouveaux fichiers dans les 2 PF

Les configurations des 2 pare-feu sont gérées par git → commit si modif OK.

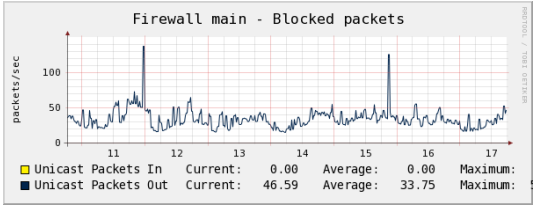
Suivi des traces et statistiques

Traces :

- Traces au format PCAP (tcpdump)
- Enregistre les paquets bloqués explicitement

Statistiques :

- Données SNMP sur les interfaces + interface virtuelle `pflog0`
- Collecteur netflow (non exploité)



Résultats

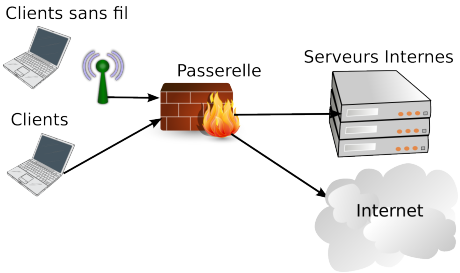
- Solution en place depuis septembre 2009
  - 2 serveurs Xeon 2.5 GHz
  - OpenBSD/amd64 4.8, 4.9 puis 5.0
- Répond aux besoins, résiste aux attaques
- Redondance OK (mises à jour et quelques tests)
- Administration améliorée : 4 personnes font des modifications dans les règles (une seule avant sur Cisco)

Agenda

Besoin

Problématique :

- Contrôler l'accès au réseau des machines des visiteurs (sans fil et filaire)
- Supporter une vaste gamme de systèmes
- Ne pas nécessiter de support/assistance
- Administration simple



Solutions

- Clé partagée WEP/WPA Personnal
  - WEP :)
  - manque de support WPA dans matériels anciens
- Authentification WPA Enterprise,...
  - supporté par drivers récents seulement
  - complexe.
  - fonctionne avec certaines populations (Eduroam...)
- Authpf
  - authentification SSH sur passerelle $\rightarrow$ ouverture pare-feu.
  - nécessite un client SSH sur les postes (peut être distribué par la passerelle)
- Portail captif
  - solution utilisée par de nombreux hotspots commerciaux
  - problème de la notion de session
  - authentification ?

Osap

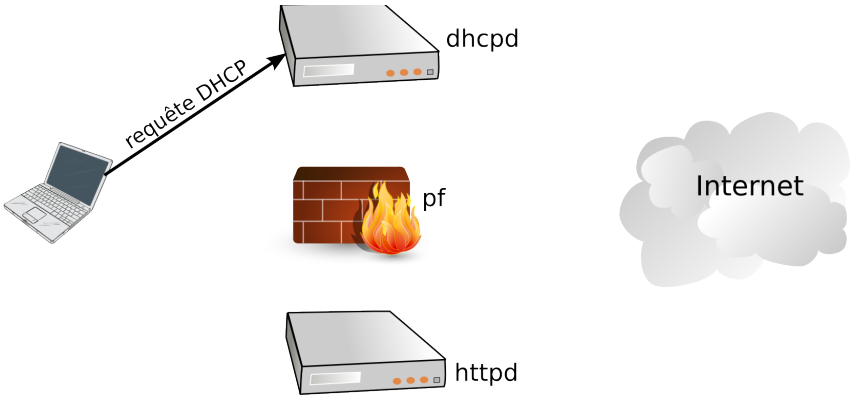
- Portail captif basé sur OpenBSD et ses outils: PF, dhcpd.
- Inspiré de authpf
- Auto-identification des utilisateurs
- Fonctionne en mode routeur.
- Écrit en Perl

Osap - principe

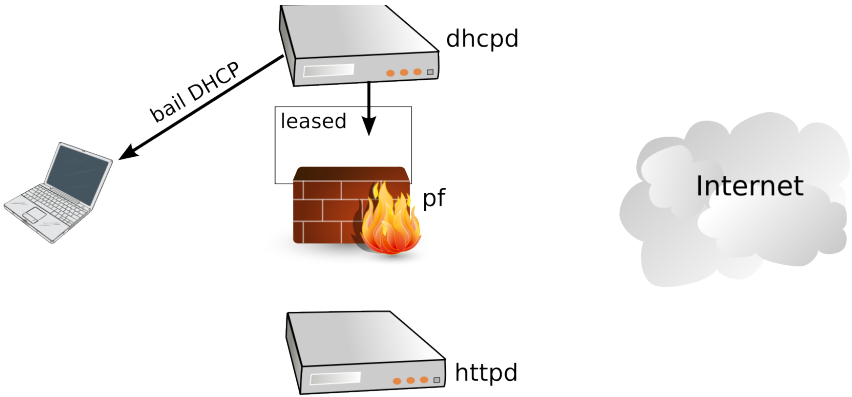
Principe:

- 3 tables PF:
  - **abandonned :** baux DHCP inactifs → trafic bloqué complètement
  - **leased :** baux DHCP actifs - pas encore authentifiés → trafic redirigé vers portail
  - **users :** baux DHCP actifs - identifiés → trafic passe normalement
- un script CGI assure l'identification. Envoie requêtes au démon `osapd` pour modification tables pf.
- `dhcpd` place automatiquement les adresses abandonnées (DHCP RELEASE, timeout) dans la table abandonned.

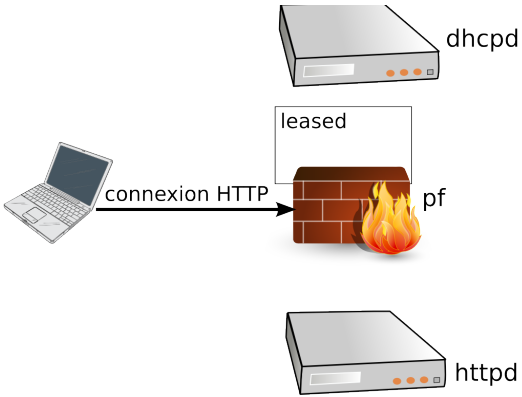
Osap - fonctionnement



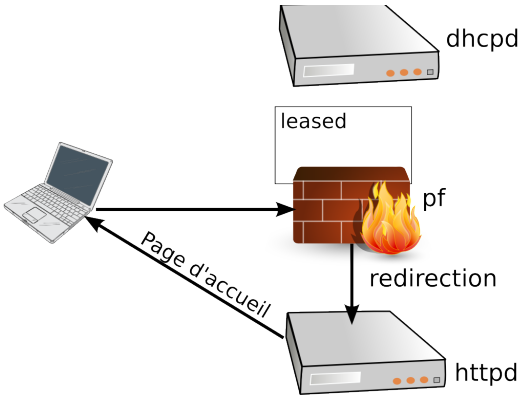
Osap - fonctionnement



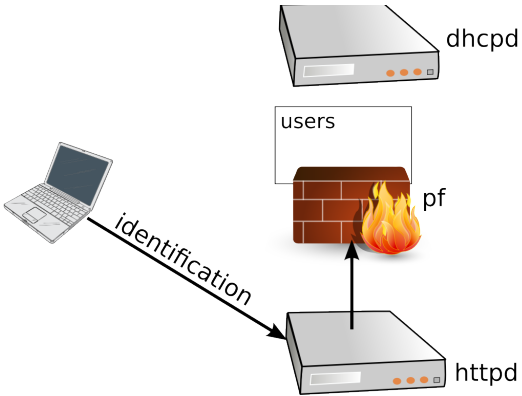
Osap - fonctionnement



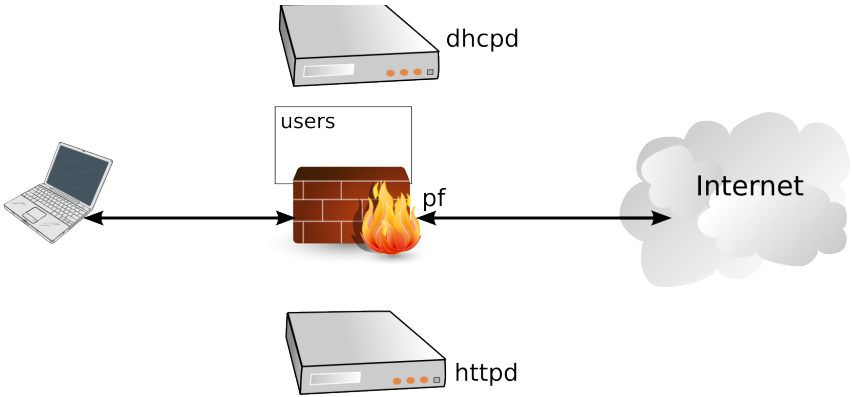
Osap - fonctionnement



Osap - fonctionnement



Osap - fonctionnement



Osap - sécurité

- Serveur DNS en mode récursif sur la passerelle : blocage complet du trafic avant identification.
- Table *abandonned* contre le squat d'adresses non utilisées.
- Fonctionnalité de dhcpd pour bloquer le squat de baux valides (place les adresses IP qui changent d'adresse MAC dans une table PF spéciale : blacklist)
- Écrit en perl: limite les risques d'erreur. Données utilisateur très contrôlées.
- Limite le trafic autorisé : HTTP[S], POP/IMAP[S], FTP, SSH, VPNs,.., pas de trafic entrant.
- Conserve pendant un an : identifiant + adresse mail, adresse IP, adresse MAC.

Bilan du portail captif

- Opérationnel depuis 3 ans
- Très utilisé (2300 connexions en octobre 2011),
- Presque pas de maintenance

Quelques problèmes :

- Utilisé comme alternative par des membres du laboratoire
- Quelques mauvaises têtes qui donnent des identités bidon (surtout des membres du laboratoire)
- Manque le support d'IPv6 :-(

Agenda

Conclusion

- Solutions efficaces et d'un coût limité,
- Permettent de maîtriser les choix techniques en fonction d'une politique de sécurité,
- Support via communauté d'utilisateurs : mutualisation intelligente productive,
- Aspects pédagogiques : comprendre et expliquer ce qui est fait,
- Ouvertes à des évolutions.

Questions ?