

Toc-toc, ouvre-moi la porte !

*Port knocking et SPA pour protéger
efficacement les accès réseau*

Par Jean-Denis GIRARD



Plan

Le problème

Sécurité système

Utilisation de firewalls

Port knocking

Single Packet Authentication

FwKnOp

Accès distant aux serveurs

Pourquoi ?

Accès distant facilite le travail des administrateurs, et améliore la disponibilité pour les utilisateurs

Comment ?

Serveur Unix: ssh, NX

Serveur Windows: VNC, TSE

Sécurité système

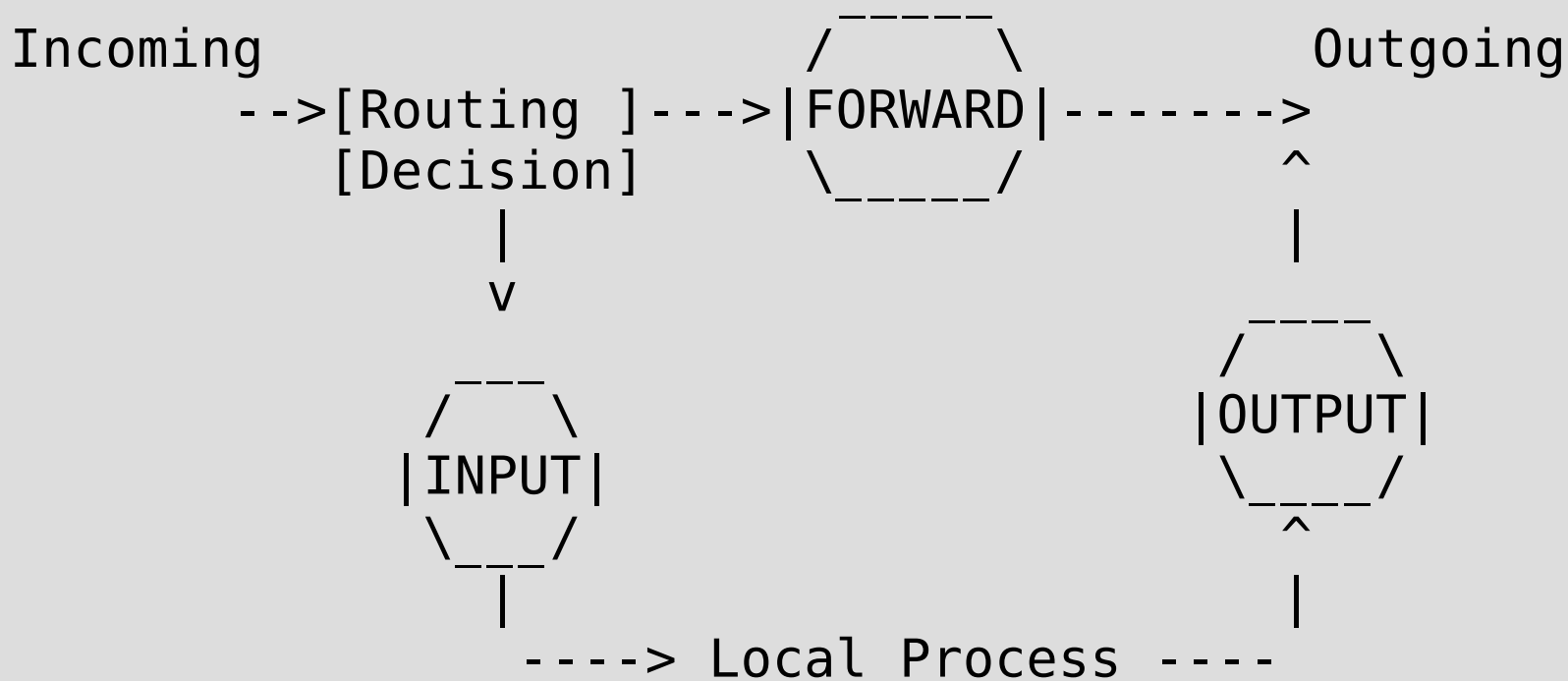
ssh : limiter le nombre d'utilisateurs autorisés (un seul ?), interdire accès root, remplacer les mots de passe par des clés.

Utiliser sudo.

Utiliser un shell restreint (rsh).

Sécurité réseau

Filtrage avec IpTables / NetFilter



```
sudo iptables -j INPUT DROP
sudo iptables -j OUTPUT DROP
sudo iptables -j FORWARD DROP
```

Restreindre les accès à la plage d'adresses du
FAI: 123.50.64.0/18, 202.3.224.0/19,
202.90.64.0/19, 203.185.160.0/20,
203.185.176.0/21

ex: sur une semaine, plus de **300 accès bloqués** par le pare feu. **Aucune** tentative d'accès illicite n'a atteint sshd !

Limites pare-feu

Même protégé par le pare-feu, le port SSH reste visible / accessible depuis les adresses autorisées:

tentation pour les pirates,

à la merci d'une faille dans sshd (ex. CVE-2003-0693, CVE-2003-0695),

à la merci d'une faille dans le système de génération des clés (ex. CVE-2008-0166 13/05/08).

Port knocking

Idée apparue en 2001, implémentation en 2003.

Wikipédia: « Le port-knocking est une méthode permettant de modifier le comportement d'un firewall en temps réel en provoquant l'ouverture de ports permettant la communication, grâce au lancement préalable d'une suite de connexions sur des ports distincts dans le bon ordre, à l'instar d'un code frappé à une porte. »

Port cible bloqué par le firewall

Un programme surveille les logs du firewall

Lorsque ce programme détecte une séquence prédéfinie de paquets, il ouvre le port cible pour l'adresse source, et pour une durée limitée.

L'administrateur peut alors se connecter.

=> Authentification niveau pare-feu

Limites port knocking

Attaque en force peut fonctionner sur un réseau rapide ($65535 \text{ ports}^3 \Rightarrow \sim 281\,000$ milliards de combinaisons)

Visible sur le réseau, notamment pour les IDS.

Attaque possible en rejouant la séquence.

Délivrance des paquets dans le désordre.

Single Packet Authentication

Apparue en 2005.

Principe similaire au port knocking, mais l'information est transmise via les données d'un unique paquet.

La quantité d'information transmissible est beaucoup plus importante.

Néanmoins plus discret sur le réseau.

Peut utiliser ICMP.

FwKnop

Implémentation libre (GPL) du principe SPA.

Serveur disponible pour Linux (iptables), *BSD et Mac OS X (ipfw).

Client disponible pour Linux, *BSD, Windows (via Cygwin).

Authentification possible par clé GPG.

Conclusion

fwknop est un outil supplémentaire pour améliorer la sécurité des accès distants.

Systeme et implémentation ouverts, publiés et étudiés: pas de réelle faiblesse découverte, ni remise en cause des principes.

Questions ?

Références

Cipherdyne

<http://www.cipherdyne.org/fwknop/>

Linux Journal (mai / août 2007)

<http://www.linuxjournal.com/article/9621>

<http://www.linuxjournal.com/article/9565>

Hervé Schauer Consultants

<http://www.hsc.fr/ressources/breves/SPA.html.fr>

Port knocking

http://fr.wikipedia.org/wiki/Port_knocking

<http://www.portknocking.org/>