HOWTO Passerelle d'Authentification

Nathan Zorn

<zornnh@musc.edu>

Guillaume Lelarge – Traduction française

Guillaume Hatt – Relecture de la version française

Historique des versions

Version 0.06	2002−11−05	Revu par : nhz
Version 0.05	2002−05−10	Revu par : nhz
Version 0.04	2002−02−28	Revu par : nhz
Version 0.03	2001−09−28	Revu par : nhz
Version 0.02	2001−09−28	Revu par : KET
Version 0.01	2001−09−06	Revu par : nhz

Beaucoup se sentent concernés par la sécurité des réseaux sans−fil et des aires d'accès public telles que les bibliothèques et les dortoirs. Les implémentations actuelles de sécurité ne répondent pas à ces interrogations. Une réponse est proposée par l'utilisation d'une passerelle d'authentification. Cette passerelle réponds aux problèmes de sécurité en forçant l'utilisateur à s'authentifier pour pouvoir utiliser le réseau.

Table des matières

1. Introduction

Avec les réseaux sans−fil et les aires d'accès publics, il est très facile pour un utilisateur non autorisé d'accéder au réseau. Les utilisateurs non autorisés peuvent chercher un signal et récupérer des informations de connexion à partir de ce signal. Ils peuvent brancher leur machine sur un terminal public et obtenir l'accès au réseau. Des éléments de sécurité ont été mis en place, comme WEP, mais cette sécurité peut être franchie avec des outils comme AirSnort. Une approche pour résoudre ces problèmes est de ne pas se reposer sur les fonctionnalités de sécurité des sans−fil, et d'installer à la place une passerelle d'authentification devant le réseau sans−fil ou les aires d'accès public, ce qui permet de forcer les utilisateurs à s'authentifier avant d'utiliser le réseau. Ce HOWTO décrit comment mettre en place cette passerelle avec Linux.

1.1. Informations de Copyright

Si vous avez des questions, merci de contacter `<zornnh@musc.edu>`

1.2. Disclaimer

Aucune responsabilité pour le contenu de ce document ne sera acceptée. Utilisez les concepts, exemples et autre contenu à vos risques et périls. Comme il s'agit d'une nouvelle édition de ce document, il peut y avoir des erreurs et des inexactitudes, qui peuvent endommager votre système. Procédez avec prudence et bien que les dégats soient très improbables, les auteurs n'en prennent aucune responsabilité.

Tous les droits sont détenus par leurs propriétaires respectifs, sauf cas spécifique indiqué. L'utilisation d'un terme dans ce document ne doit pas être vu comme affectant la validité d'une marque ou d'un service.

Nommer un produit particulier ou une marque ne doit pas être vu comme une illégalité.

Il est fortement conseillé de faire une sauvegarde de votre système avant toute installation majeure, et d'en faire à intervalles réguliers.

1.3. Nouvelles Versions

La version la plus récente de ce document peut être trouvée sur . Les HOWTOs en rapport peuvent être trouvés sur le site Linux Documentation Project .

1.4. Crédits

Jamin W. Collins

Kristin E Thomas

Logu (visolve.com)

1.5. Retour d'informations

Le retour d'informations est vraiment bienvenu pour ce document. Sans vos soumissions, ce document n'existerait pas. Merci d'envoyer vos ajouts, commentaires et critiques à l'adresse mail suivante : `<zornnh@musc.edu>`.

2. Ce qui est nécessaire

Cette section décrit ce qui est nécessaire pour installer la passerelle d'authentification.

2.1. Netfilter

La passerelle d'authentification utilise Netfilter et iptables pour gérer le pare−feu. Consultez le HOWTO Netfilter .

2.2. Logiciel pour les règles dynamiques de Netfilter

Un moyen pour insérer et supprimer des règles Netfilter est d'utiliser pam_iptables. Il s'agit d'un module d'authentification insérable (PAM ou « pluggable authentication module ») écrit par Nathan Zorn disponible sur . Ce module PAM permet aux utilisateurs d'utiliser ssh et telnet pour s'authentifier sur la passerelle.

Un autre moyen pour supprimer et créer dynamiquement des règles Netfilter est d'utiliser NocatAuth. Il peut être trouvé sur . NocatAuth fournit un client web pour s'authentifier sur la passerelle.

2.3. Serveur DHCP

La passerelle d'authentification agira comme un serveur DHCP (« Dynamic Host Configuration Protocol ») pour le réseau public. Elle sert seulement ceux qui réclament des services DHCP sur le réseau public. J'ai utilisé le serveur DHCP ISC.

2.4. Mécanisme d'authentification

La passerelle peut utiliser tous les moyens d'authentification de PAM. L'université de médecine de Caroline du Sud utilise LDAP comme mécanisme d'authentification. Comme LDAP a été utilisé pour l'authentification, les modules pam sur la machine passerelle ont été configurés pour utiliser LDAP. D'autres informations sont disponibles sur . PAM vous permet d'utiliser beaucoup de moyens d'authentification. Merci de regarder la documentation pour le module PAM que vous souhaitez utiliser. Pour plus d'informations sur les autres méthodes, voir les modules pam correspondants.

Si NocatAuth est utilisé, un service d'authentification a besoin d'être configuré. Le service d'authentification NocatAuth supporte l'authentification avec LDAP, RADIUS, MySQL et un fichier de mots de passe. Plus d'informations sur la page .

2.5. Serveur DNS

La machine passerelle sert aussi de serveur DNS pour le réseau public. J'ai installé Bind, et je l'ai configuré comme un serveur de noms cache. Le paquetage rpm caching−nameserver a aussi été utilisé. Ce paquetage provient de RedHat.

3. Configuration des services de la passerelle

Cette section décrit comment configurer chaque pièce de la passerelle d'authentification. Les exemples utilisés concernent un réseau public compris dans le sous−réseau 10.0.1.0. eth0 est l'interface connectée au réseau interne. eth1 est l'interface connecté au réseau public. L'adresse IP utilisée pour cette interface est 10.0.1.1. Ces valeurs peuvent être changées pour s'intégrer au réseau que vous utilisez. RedHat 7.1 a été utilisé pour la machine passerelle, donc un grand nombre d'exemples sont spécifiques à RedHat.

3.1. Configuration de Netfilter

Pour configurer netfilter, le noyau doit être recompilé pour inclure le support de netfilter. Merci de consulter le HOWTO Noyau pour plus d'informations sur la configuration et la compilation de votre noyau.

Voici à quoi ressemble la configuration de mon noyau.

```
#
# Networking options
#
CONFIG_PACKET=y
# CONFIG_PACKET_MMAP is not set
# CONFIG_NETLINK is not set
CONFIG_NETFILTER=y
CONFIG_NETFILTER_DEBUG=y
CONFIG_FILTER=y
CONFIG_UNIX=y
CONFIG_INET=y
CONFIG_IP_MULTICAST=y
# CONFIG_IP_ADVANCED_ROUTER is not set
# CONFIG_IP_PNP is not set
# CONFIG_NET_IPIP is not set
# CONFIG_NET_IPGRE is not set
# CONFIG_IP_MROUTE is not set
# CONFIG_INET_ECN is not set
# CONFIG_SYN_COOKIES is not set


#   IP: Netfilter Configuration
#
CONFIG_IP_NF_CONNTRACK=y
CONFIG_IP_NF_FTP=y
CONFIG_IP_NF_IPTABLES=y
CONFIG_IP_NF_MATCH_LIMIT=y
CONFIG_IP_NF_MATCH_MAC=y
CONFIG_IP_NF_MATCH_MARK=y
CONFIG_IP_NF_MATCH_MULTIPORT=y
CONFIG_IP_NF_MATCH_TOS=y
CONFIG_IP_NF_MATCH_TCPMSS=y
CONFIG_IP_NF_MATCH_STATE=y
CONFIG_IP_NF_MATCH_UNCLEAN=y
CONFIG_IP_NF_MATCH_OWNER=y
CONFIG_IP_NF_FILTER=y
CONFIG_IP_NF_TARGET_REJECT=y
CONFIG_IP_NF_TARGET_MIRROR=y
CONFIG_IP_NF_NAT=y
CONFIG_IP_NF_NAT_NEEDED=y
CONFIG_IP_NF_TARGET_MASQUERADE=y
CONFIG_IP_NF_TARGET_REDIRECT=y
CONFIG_IP_NF_NAT_FTP=y
CONFIG_IP_NF_MANGLE=y
CONFIG_IP_NF_TARGET_TOS=y
CONFIG_IP_NF_TARGET_MARK=y
```

```
CONFIG_IP_NF_TARGET_LOG=y
CONFIG_IP_NF_TARGET_TCPMSS=y
```

Une fois que netfilter a été configuré, mettez en place la transmission IP (IP forwarding) en exécutant cette commande :

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Pour s'assurer que la transmission ip est activée lors du redémarrage de la machine, ajoutez la ligne suivante dans `/etc/sysctl.conf` :

```
net.ipv4.ip_forward = 1
```

Si vous allez utilisé NocatAuth, vous pouvez passer à la section Configuration de la passerelle NoCatAuth.

Iptables a besoin d'être installé. Pour cela, soit vous utilisez le paquetage provenant de votre distribution, soit vous l'installez à partir des sources. Une fois que les options ci−dessus ont été compilées dans le nouveau noyau et qu'iptables a été installé, je mets en place les règles par défaut du pare−feu.

```
iptables −t nat −A POSTROUTING −o eth0 −j MASQUERADE
iptables −A INPUT −i eth0 −m state −−state NEW, INVALID −j DROP
iptables −A FORWARD −i eth0 −m state −−state NEW, INVALID −j DROP
iptables −I FORWARD −o eth0 −j DROP
iptables −I FORWARD −s 10.0.1.0/24 −d 10.0.1.1 −j ACCEPT
```

Les commandes ci−dessus peuvent aussi être placées dans un script d'initialisation utilisé lorsque le serveur redémarre. Pour s'assurer que les règles ont été ajoutées, tapez les commandes suivantes :

```
iptables −v −t nat −L
iptables −v −t filter −L
```

Pour sauvegarder ces règles, j'ai utilisé les scripts d'initialisation de RedHat.

```
/etc/init.d/iptables save
/etc/init.d/iptables restart
```

Maintenant, la machine passerelle est capable de faire de la traduction d'adresses réseau (NAT ou Network Address Translation), mais elle laissera passer tous les paquets sauf ceux provenant de l'intérieur du réseau public et à destination de la passerelle.

3.2. Règles dynamiques de Netfilter.

Cette section décrit comment configurer le logiciel nécessaire à l'insertion et à la suppression dynamique de règles Netfilter sur la passerelle.

3.2.1. Module iptables pour PAM

Le module de session PAM, qui insère les règles pour le pare−feu, est nécessaire pour permettre la transmission pour le client authentifié. Pour le configurer, récupérez simplement le fichier source et compilez−le en lançant les commandes suivantes :

```
  gcc −fPIC −c pam_iptables.c
  ld −x −−shared −o pam_iptables.so pam_iptables.o
```

Vous devez maintenant avoir deux binaires appelés `pam_iptables.so` et `pam_iptables.o`. Copiez `pam_iptables.so` dans `/lib/security/pam_iptables.so` :

```
cp pam_iptables.so /lib/security/pam_iptables.so
```

Maintenant, installez le script pare−feu dans le répertoire /usr/local/auth−gw :

```
mkdir /usr/local/auth-gw
cp insFwall /usr/local/auth-gw
```

Le client d'authentification choisi pour la passerelle étant ici ssh, nous avons ajouté la ligne suivante dans `/etc/pam.d/sshd` :

```
session    required     /lib/security/pam_iptables.so
```

Maintenant, lorsqu'un utilisateur se connectera avec ssh, la règle du pare−feu sera ajoutée.

Pour savoir si le module pam_iptables fonctionne, réalisez les étapes suivantes :

1. Connectez−vous sur la machine avec ssh.
2. Vérifiez si la règle a été ajoutée avec la commande **iptables −L −v**.
3. Déconnectez−vous de la machine pour vous assurer que la règle est bien supprimée.

3.2.2. Passerelle NoCatAuth

Cette section décrit le processus de configuration de la passerelle NocatAuth. Pour la configurer, récupérez le source et installez−le avec les étapes suivantes.

Assurez−vous que gpgv est installé. gpgv est un vérificateur de signatures PGP. Il fait partie de gnupg et peut être trouvé sur la page http://www.gnupg.org/download.html.

Extrayez les fichiers de l'archive tar NocatAuth :

```
tar xvzf NocatAuth-x.xx.tar.gz
```

Si vous ne voulez pas que NocatAuth soit installé dans le répertoire /usr/local/nocat, éditez le Makefile et remplacez INST_PATH par le répertoire où vous souhaitez que NoCatAuth soit installé.

Puis, construisez la passerelle :

```
cd NoCatAuth-x.xx
make gateway
```

Editez le fichier /usr/local/nocat.conf. Merci de consulter le fichier de documentation INSTALL pour les détails sur ce qui est requis dans le fichier de configuration. Un fichier de configuration d'exemple ressemble à ceci :

```
###### gateway.conf -- NoCatAuth Gateway Configuration.
#
# Format of this file is: Directive Value, one per
# line. Trailing and leading whitespace is ignored. Any
# line beginning with a punctuation character is assumed to
# be a comment.

Verbosity       10
#we are behind a NAT so put the gateway in passive mode
```

```
GatewayMode     Passive
GatewayLog      /usr/local/nocat/nocat.log
LoginTimeout    300

######Open Portal settings.
HomePage        http://www.itlab.musc.edu/
DocumentRoot    /usr/local/nocat/htdocs
SplashForm      splash.html
###### Active/Passive Portal settings.
TrustedGroups Any
AuthServiceAddr egon.itlab.musc.edu
AuthServiceURL  https://$AuthServiceAddr/cgi-bin/login
LogoutURL       https://$AuthServiceAddr/forms/logout.html
###### Other Common Gateway Options.
AllowedWebHosts egon.itlab.musc.edu
ResetCmd        initialize.fw
PermitCmd       access.fw permit $MAC $IP $Class
DenyCmd         access.fw deny $MAC $IP $Class
```

Maintenant, vous devez être capable de lancer la passerelle. Si un problème survient, merci de consulter la documentation INSTALL dans le répertoire NoCatAuth. La commande suivante lance la passerelle :

```
/usr/local/nocat/bin/gateway
```

3.3. Configuration du serveur DHCP

J'ai installé DHCP en utilisant le fichier `dhcpd.conf` suivant :

```
subnet 10.0.1.0 netmask 255.255.255.0 {
# --- default gateway
     option routers                  10.0.1.1;
     option subnet-mask              255.255.255.0;
     option broadcast-address        10.0.1.255;

     option domain-name-servers       10.0.1.1;
     range   10.0.1.3 10.0.1.254;
     option time-offset              -5;     # Eastern Standard Time

     default-lease-time 21600;
     max-lease-time 43200;

 }
```

Le serveur a ensuite été lancé en utilisant eth1, l'interface connectée au réseau public :

```
/usr/sbin/dhcpd eth1
```

3.4. Configuration de la méthode d'authentification

L'authentification avec PAM et un service d'authentification NoCatAuth ont été décrits. Les deux exemples utilisent LDAP. D'autres moyens d'authentification en dehors de LDAP peuvent être utilisés. Merci de lire la documentation sur PAM et NoCatAuth pour trouver les étapes nécessaires pour utiliser d'autres sources d'authentification.

3.4.1. PAM LDAP

Comme indiqué dans les sections précédentes, j'ai configuré cette passerelle pour utiliser LDAP comme moyen d'authentification. Néanmoins, vous pouvez utiliser tout autre moyen autorisé par PAM pour l'authentification. Voir Section 2.4 pour plus d'informations.

Pour obtenir l'authentification par PAM LDAP, j'ai installé OpenLDAP et je l'ai configuré avec les lignes suivantes dans `/etc/ldap.conf` :

```
# Your LDAP server. Must be resolvable without using LDAP.
host itc.musc.edu

# The distinguished name of the search base.
base dc=musc,dc=edu
ssl no
```

Les fichiers suivants ont été utilisés pour configurer PAM pour qu'il assure l'authentification LDAP. Ces fichiers ont été générés par l'utilitaire de configuration de RedHat.

`/etc/pam.d/system-auth` a été créé et ressemble à ceci :

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      /lib/security/pam_env.so
auth        sufficient    /lib/security/pam_unix.so likeauth nullok
auth        sufficient    /lib/security/pam_ldap.so use_first_pass
auth        required      /lib/security/pam_deny.so

account     required      /lib/security/pam_unix.so
account     [default=ok user_unknown=ignore service_err=ignore \
             system_err=ignore] /lib/security/pam_ldap.so

password    required      /lib/security/pam_cracklib.so retry=3
password    sufficient    /lib/security/pam_unix.so nullok use_authtok
password    sufficient    /lib/security/pam_ldap.so use_authtok
password    required      /lib/security/pam_deny.so

session     required      /lib/security/pam_limits.so
session     required      /lib/security/pam_unix.so
session     optional      /lib/security/pam_ldap.so
```

Ensuite, le fichier `/etc/pam.d/sshd` a été créé :

```
#%PAM-1.0
auth       required     /lib/security/pam_stack.so service=system-auth
auth       required     /lib/security/pam_nologin.so
account    required     /lib/security/pam_stack.so service=system-auth
password   required     /lib/security/pam_stack.so service=system-auth
session    required     /lib/security/pam_stack.so service=system-auth
#this line is added for firewall rule insertion upon login
session    required     /lib/security/pam_iptables.so debug
session    optional     /lib/security/pam_console.so
```

3.4.2. Le service NoCatAuth

Il est recommandé d'installer le service NoCatAuth sur un autre serveur, à côté de la passerelle. Un serveur séparé a été utilisé dans mes exemples. Pour configurer un service NoCatAuth, vous aurez besoin des logiciels suivants :

1. Un serveur web avec SSL activé, de préférence avec un certificat SSL enregistré. J'ai utilisé Apache avec mod_ssl.
2. Perl 5 (5.6 ou ultérieur recommandé)
3. Les modules perl Net::LDAP, Digest::MD5, DBI et DBD::MySQL (récupérez−les à partir de CPAN). Le module dont vous avez besoin dépend de la source d'authentification que vous comptez utiliser. Dans mon exemple, Net::LDAP a été utilisé comme moyen d'authentification.
4. Gnu Privacy Guard (gnupg 1.0.6 ou ultérieur), disponible sur http://www.gnupg.org/download.html

Pour l'installer, décompressez le fichier tar :

```
$ tar zvxf NoCatAuth-x.xx.tar.gz
```

Si vous souhaitez changer le chemin où réside NoCatAuth, éditez le Makefile et remplacez INST_PATH par le répertoire souhaité.

Ensuite, lancez la commande : **make authserv** . Cela installe tout dans /usr/local/nocat ou le répertoire que désigne INST_PATH.

Ensuite, lancez **make pgpkey** . Les valeurs par défaut conviennent pour la plupart des usages. IMPORTANT : n'entrez PAS de phrase (passphrase) ! Sinon, vous obtiendrez des messages étranges lorsque le service auth essaiera de crypter les messages et essaiera de lire votre phrase à partir d'un terminal tty inexistant.

Editez `/usr/local/nocat/nocat.conf` pour l'adapter à votre situation. Voici un exemple :

```
###### authserv.conf -- NoCatAuth Authentication Service Configuration.
#
# Format of this file is: Directive Value, one per
#   line. Trailing and leading whitespace is ignored. Any
#   line beginning with a punctuation character is assumed to
#   be a comment.

Verbosity       10
HomePage        http://www.itlab.musc.edu/
DocumentRoot    /usr/local/nocat/htdocs
# LDAP source
DataSource LDAP
LDAPHost authldap.musc.edu
LDAPBase dc=musc,dc=edu

UserTable       Member
UserIDField     User
UserPasswdField Pass
UserAuthField   Status
UserStampField  Created

GroupTable      Network
GroupIDField    Network
GroupAdminField Admin
MinPasswdLength 8

# LocalGateway -- If you run auth service on the same subnet
#   (or host) as the gateway you need to specify the hostname
#   of the gateway. Otherwise omit it.  (Requires Net::Netmask)
#
# LocalGateway    192.168.1.7

LoginForm       login.html
LoginOKForm     login_ok.html
FatalForm       fatal.html
ExpiredForm     expired.html
RenewForm       renew.html
```

```
PassiveRenewForm renew_pasv.html
RegisterForm    register.html
RegisterOKForm  register_ok.html
RegisterFields  Name URL Description

UpdateForm      update.html
UpdateFields    URL Description

###### Auth service user messages. Should be self-explanatory.
#
LoginGreeting   Greetings! Welcome to the Medical University of SC's Network.
LoginMissing    Please fill in all fields!
LoginBadUser    That e-mail address is unknown. Please try again.
LoginBadPass    That e-mail and password do not match. Please try again.
LoginBadStatus  Sorry, you are not a registered co-op member.

RegisterGreeting    Welcome! Please enter the following information to register.
RegisterMissing     Name, E-mail, and password fields must be filled in.
RegisterUserExists  Sorry, that e-mail address is already taken. Are you already registered?
RegisterBadUser     The e-mail address provided appears to be invalid. Did you spell it correc
RegisterInvalidPass All passwords must be at least six characters long.
RegisterPassNoMatch The passwords you provided do not match. Please try again.
RegisterSuccess     Congratulations, you have successfully registered.

UpdateGreeting      Enter your E-mail and password to update your info.
UpdateBadUser       That e-mail address is unknown. Please try again.
UpdateBadPass       That e-mail and password do not match. Please try again.
UpdateInvalidPass   New passwords must be at least eight characters long.
UpdatePassNoMatch   The new passwords you provided do not match. Please try again.
UpdateSuccess       Congratulations, you have successfully updated your account.
```

Assurez–vous que le répertoire /usr/local/nocat/pgp appartient à l'utilisateur du serveur web (c'est–à–dire nobody ou www–data).

Ajoutez etc/authserv.conf à votre fichier apache `httpd.conf`.

```
Include /usr/local/nocat/etc/authserv.conf
```

Copiez votre /usr/local/nocat/trustedkeys.pgp sur la passerelle. Relancez Apache et essayez. Merci de vous reporter à la documentation de NoCatAuth pour plus d'informations. Elle est disponible dans le répertoire docs/ de l'archive NoCatAuth décompressée.

3.5. Configuration du DNS

J'ai installé la version par défaut de Bind fournie avec RedHat 7.1 et le paquetage RPM du serveur de noms cache. Le serveur DHCP indique aux machines du réseau public d'utiliser la machine passerelle comme serveur de noms.

4. Utiliser la passerelle d'authentification

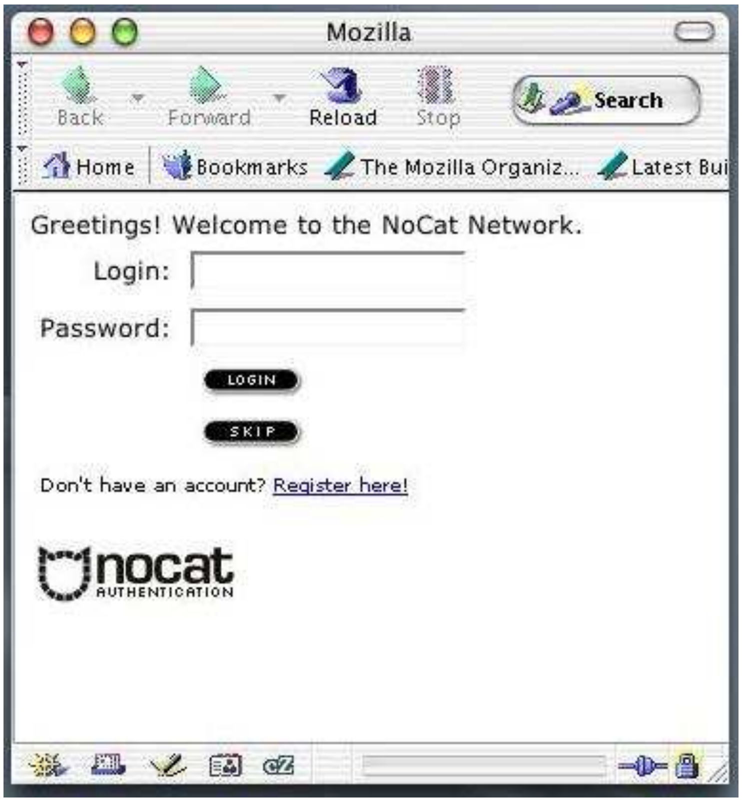
Pour utiliser la passerelle d'authentification, configurez votre machine client pour l'usage du DHCP. Installez un client ssh sur la machine et connectez–vous avec ssh sur la passerelle. Une fois connecté, vous aurez accès au réseau interne. Ce qui suit est une session exemple à partir d'un client unix :

```
bash>ssh zornnh@10.0.1.1
zornnh's Password:

gateway>
```

Aussi longtemps que vous restez connecté, vous y aurez accès. Une fois déconnecté, l'accès sera fermé.

Pour utiliser la passerelle d'authentification avec NoCatAuth, configurez votre machine client pour l'usage du DHCP. Installez un navigateur web tel que Mozilla. Lancez le navigateur web qui devra être redirigé sur l'écran d'authentification.



Connexion à partir de Nocat

Indiquez votre nom d'utilisateur et votre mot de passe. Une fenêtre s'ouvrira pour vous expliquer que vous êtes authentifié sur le réseau et que vous devez conserver la fenêtre ouverte pour le rester. Cliquez sur logout ou fermez la fenêtre pour terminer la session.

Fenêtre d'authentification

5. Remarques de conclusion

- Cette méthode de sécurisation ne dépend pas de la sécurité apportée par la communauté du réseau sans−fil. Elle part du principe que le réseau sans−fil dans son intégralité est non sécurisé et situé en

dehors de votre réseau.
- La passerelle ne crypte pas le trafic. Elle vous permet seulement d'accéder au réseau situé derrière elle. Si vous désirez le cryptage et l'authentification, vous devriez utiliser un VPN.

6. Ressources supplémentaires

- Un document décrivant l'implémentation d'une passerelle d'authentification à la NASA.
- Un livre blanc décrivant comment l'Université d'Alberta a créé une passerelle d'authentification.
- Nocat.net a une passerelle d'authentification pour les réseaux sans−fil. Ce logiciel dispose d'un client web.
- Horatio : Authenticated Network Access est un outil pare−feu d'authentification. Leur idée : les utilisateurs légitimes veulent attacher des portables et autres hôtes mobiles au réseau, mais la sécurité demande que les utilisateurs illégitimes n'aient ni la possibilité d'accèder au réseau interne et sécurisé, ni celle d'abuser d'Internet.

7. Questions et réponses

C'est juste un rassemblement de toutes les questions les plus courantes à ma connaissance. Apportez−moi un retour d'informations pour que je puisse transformer cette section en une vrai FAQ.

1. Pourquoi les règles d'iptables ne sont−elles pas supprimées quand un client quitte une fenêtre telnet ? Cela fonctionne si le client se déconnecte de la session telnet. Dans le cas de ssh, les règles sont même supprimées si la fenêtre ssh est fermée.

   Je ne suis pas encore arrivé à une bonne réponse ou à une solution correcte à ce problème. Logu a apporté quelques modifications à pam_iptables et a créé un ensemble d'autres outils pour résoudre ce problème. Ces outils peuvent être trouvés dans le répertoire contrib avec pam_iptables.
2. Pourquoi NoCat ne fonctionne−t'il pas avec IE6 ? Il semble faire l'authentification mais n'écrit pas la règle du pare−feu.

   Assurez−vous que votre html nocat contient ce qui suit : <meta http−equiv="Refresh" content="$redirect"/>

   Les fichiers html qui contiennent ce metatag sont login_ok.html, renew.html, et renew_pasv.html.

8. Adaptation française

8.1. Traduction

La traduction française de ce document a été réalisée par Guillaume Lelarge <`gleu@wanadoo.fr`>.

8.2. Relecture

La relecture de ce document a été réalisée par Guillaume Hatt <`ghatt@netcourrier.com`>.