Authentication Gateway HOWTO

Nathan Zorn

zornnh@musc.edu

Revision History

Revision 0.05 2002-11-05 Revised by: nhz

Revision 0.05 2002-05-10 Revised by: nhz

Revision 0.04 2002-02-28 Revised by: nhz

Revision 0.03 2001-09-28 Revised by: nhz

Revision 0.02 2001-09-28 Revised by: KET

Revision 0.01 2001-09-06 Revised by: nhz

There are many concerns with the security of wireless networks and public access areas such as libraries or dormitories. These concerns are not met with current security implementations. A work around has been proposed by using an authentication gateway. This gateway addresses the security concerns by forcing the user to authenticate in order to use the network.

1. Introduction

With wireless networks and public acces areas it is very easy for an unauthorized user to gain access. Unauthorized users can look for a signal and grab connection information from the signal. Unauthorized users can plug their machine into a public terminal and gain access to the network. Security has been put in place such as WEP, but this security can be subverted with tools like AirSnort. One approach to solving these problems is to not rely on the wireless security features , and instead to place an authentication gateway in front of the wireless network or public access area and force users to authenticate against it before using the network. This HOWTO describes how to set up this gateway with Linux.

1.1. Copyright Information

If you have any questions, please contact <zornnh@musc.edu>

1.2. Disclaimer

No liability for the contents of this documents can be accepted. Use the concepts, examples and other content at your own risk. As this is a new edition of this document, there may be errors and inaccuracies, that may of course be damaging to your system. Proceed with caution, and although this is highly unlikely, the author(s) do not take any responsibility for that.

All copyrights are held by their by their respective owners, unless specifically noted otherwise. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Naming of particular products or brands should not be seen as endorsements.

You are strongly recommended to take a backup of your system before major installation and backups at regular intervals.

1.3. New Versions

The newest release of this document can be found at http://www.itlab.musc.edu/~nathan/authentication_gateway/ (http://www.itlab.musc.edu/~nathan/authentication_gateway/). Related HOWTOs can be found at the Linux Documentation Project (http://www.linuxdoc.org/) homepage.

1.4. Credits

Jamin W. Collins

Kristin E Thomas

Logu (visolve.com)

1.5. Feedback

Feedback is most certainly welcome for this document. Without your submissions and input, this document wouldn't exist. Please send your additions, comments and criticisms to the following email address : <zornnh@musc.edu>.

2. What is needed

This section describes what is needed for the authentication gateway.

2.1. Netfilter

The authentication gateway uses Netfilter and iptables to manage the firewall. Please see the Netfilter HOWTO (http://netfilter.samba.org/unreliable-guides/packet-filtering-HOWTO/index.html).

2.2. Software for dynamic Netfilter rules.

One means to insert and remove Netfilter rules is to use pam_iptables. This is a pluggable authentication module (PAM) written by Nathan Zorn that can be found at http://www.itlab.musc.edu/~nathan/pam_iptables (http://www.itlab.musc.edu/~nathan/pam_iptables/). This PAM module allows users to use ssh and telnet to authenticate to the gateway.

Another means to dynamically remove and create Netfilter rules is to use NocatAuth. NocatAuth can be found at http://nocat.net (http://nocat.net). NocatAuth provides a web client for authenticating to the gateway.

2.3. DHCP Server

The authentication gateway will act as the dynamic host configuration protocol (DHCP) server for the public network. It only serves those requesting DHCP services on the public network. I used the ISC DHCP Server (http://www.isc.org/products/DHCP/).

2.4. Authentication mechanism

The gateway can use any means of PAM authentication. The authentication mechanism the Medical University of South Carolina uses is LDAP. Since LDAP was used for authentication, the pam modules on the gateway box were set up to use LDAP. More information can be found at http://www.padl.com/pam_ldap.html (http://www.padl.com/pam_ldap.html). PAM allows you to use many means of authentication. Please see the documentation for the PAM module you would like to use. For more information on other methods, see pam modules (http://www.kernel.org/pub/linux/libs/pam/modules.html).

If NocatAuth is used, an authentication service needs to be setup. The NocatAuth authentication service supports authentication with LDAP,RADIUS,MySQL,and a password file. More information can be found at http://nocat.net/download/NoCatAuth/ (http://nocat.net/download/NoCatAuth/).

2.5. DNS Server

The gateway box also serves as a DNS server for the public network. I installed Bind (http://www.isc.org/products/BIND/), and set it up as a caching nameserver. The rpm package caching-namserver was also used. This package came with Red Hat.

3. Setting up the Gateway Services

This section describes how to setup each piece of the authentication gateway. The examples used are for a public network in the 10.0.1.0 subnet. eth0 is the interface on the box that is connected to the internal network. eth1 is the interface connected to the public network. The IP address used for this interface is 10.0.1.1. These settings can be changed to fit the network you are using. Red Hat 7.1 was used for the gateway box, so a lot of the examples are specific to Red Hat.

3.1. Netfilter Setup

To setup netfilter the kernel must be recompiled to include netfilter support. Please see the Kernel-HOWTO (http://www.linuxdoc.org/HOWTO/Kernel-HOWTO.html) for more information on configuring and compiling your kernel.

This is what my kernel configuration looked like.

```
#
# 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
```

Once netfilter has been configured, turn on IP forwarding by executing this command.

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

To make sure ip forwarding is enabled when the machine restarts add the following line to `/etc/sysctl.conf`.

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

If NocatAuth is being used, you can skip to the NoCatAuth gateway setup section.

iptables needs to be installed. To install iptables either use a package from your distribution or install from source. Once the above options were compiled in the new kernel and iptables was installed, I set the following default firewall rules.

```
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
```

The above commands can also be put in an initscript to start up when the server restarts. To make sure the rules have been added issue the following commands:

```
iptables -v -t nat -L
iptables -v -t filter -L
```

To save these rules I used Red Hat's init scripts.

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

Now the gateway box will be able to do network address translation (NAT), but it will drop all forwarding packets except those coming from within the public network and bound for the gateway.

3.2. Dynamic Netfilter rules.

This section describes how to setup the software needed to dynamically insert and remove Netfilter rules on the gateway.

3.2.1. PAM iptables Module

The PAM session module that inserts the firewall rules is needed to allow forwarding for the authenticated client. To set it up simply get the source (ftp://ftp.itlab.musc.edu/pub/pam_iptables.tar.gz) and compile it by running the following commands.

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

You should now have two binaries called `pam_iptables.so` and `pam_iptables.o`. Copy `pam_iptables.so` to `/lib/security/pam_iptables.so`.

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

Now install the firewall script to /usr/local/auth-gw.

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

The chosen authentication client for the gateway was ssh so we added the following line to `/etc/pam.d/sshd`.

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

Now, when a user logs in with ssh, the firewall rule will be added.

To test if the pam_iptables module is working perform the following steps:

1. Log into the box with ssh.
2. Check to see if the rule was added with the command **iptables -L -v**.
3. Log out of the box to make sure the rule is removed.

3.2.2. NoCatAuth gateway

This section describes the process of setting up the NocatAuth gateway. To setup NocatAuth get the source (http://nocat.net/download/NoCatAuth/) and install with the following steps.

Make sure gpgv is installed. gpgv is a PGP signature verifier. It is part of gnupg and can be found at http://www.gnupg.org/download.html.

Unpack the NocatAuth tar file.

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

If you do not want NoCatAuth to be in the directory /usr/local/nocat, edit the Makefile and change INST_PATH to the directory you would like NoCatAuth to reside.

Next build the gateway.

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

Edit the /usr/local/nocat.conf file. Please see the INSTALL documentation for details on what is required in the conf file. An example conf file looks like the following:

```
###### 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
```

Now you should be able to start the gateway. If any problems occur, please see the INSTALL documentation in the unpacked NoCatAuth directory. The following command will start the gateway:

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

3.3. DHCP Server Setup

I installed DHCP using the following `dhcpd.conf` file.

```
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;

 }
```

The server was then run using eth1 , the interface to the public net.

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

3.4. Authentication Method Setup

Authentication with PAM and a NoCatAuth authentication service is described. Both examples are done with LDAP. Other means of authentication besides LDAP can be used. Please read the documentation for PAM and NoCatAuth to find the steps to use another authentication source.

3.4.1. PAM LDAP

As indicated in previous sections, I've set this gateway up to use LDAP for authenticating. However, you can use any means that PAM allows for authentication. See Section 2.4 for more information.

In order to get PAM LDAP to authenticate, I installed OpenLDAP (http://www.openldap.org) and configured it with the following in `/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
```

The following files were used to configure PAM to do the LDAP authentication. These files were generated by Red Hat's configuration utility.

`/etc/pam.d/system-auth` was created and looked like this.

```
#%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]

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
```

Then the following `/etc/pam.d/sshd` file was created.

```
#%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. NoCatAuth Service

It is recommended to install the NoCatAuth Service on another server besides the gateway. A seperate server was used in my examples. In order to setup a NoCatAuth Service, you will need the following software:

1. An SSL enabled webserver, preferably with a registered SSL cert. I used Apache + mod_ssl.
2. Perl 5 (5.6 or better recommended)

3. Net::LDAP, Digest::MD5, DBI, and DBD::MySQL perl modules (get them from CPAN) The module you need depends on what authentication source you are going to use. In my example Net::LDAP is used as the authentication means.
4. Gnu Privacy Guard (gnupg 1.0.6 or better), available at http://www.gnupg.org/download.html

To install unpack the tar file.

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

If you would like to change the path that NoCatAuth resides , edit the Makefile and change INST_PATH to the desired directory.

Next run the command: **make authserv** This installs everything in /usr/local/nocat or what you changed INST_PATH to.

Then run **make pgpkey** The defaults should be fine for most purposes. IMPORTANT: do NOT enter a passphrase! Otherwise, you will get strange messages when the auth service attempts to encrypt messages, and tries to read your passphrase from a non-existent tty

Edit /usr/local/nocat/nocat.conf to fit your situation. Here is an example:

```
###### 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.Registe
RegisterUserExists  Sorry, that e-mail address is already taken. Are you already regist
RegisterBadUser     The e-mail address provided appears to be invalid. Did you spell it
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.
```

Make sure /usr/local/nocat/pgp is owned by the web server user. (ie..nobody or www-data)

Add etc/authserv.conf to your apache httpd.conf file.

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

Copy your /usr/local/nocat/trustedkeys.pgp to the gateway. Restart apache and try it out. Please see the NoCatAuth documentation for more information. It can be found in docs/ in the unpacked NoCatAuth directory.

3.5. DNS Setup

I installed the default version of Bind that comes with Red Hat 7.1, and the caching-nameserver RPM. The DHCP server tells the machines on the public net to use the gateway box as their nameserver.

4. Using the authentication gateway

To use the authentication gateway, configure your client machine to use DHCP. Install a ssh client on the box and ssh into the gateway. Once you are logged in, you will have access to the internal network. The following is an example session from a unix based client:

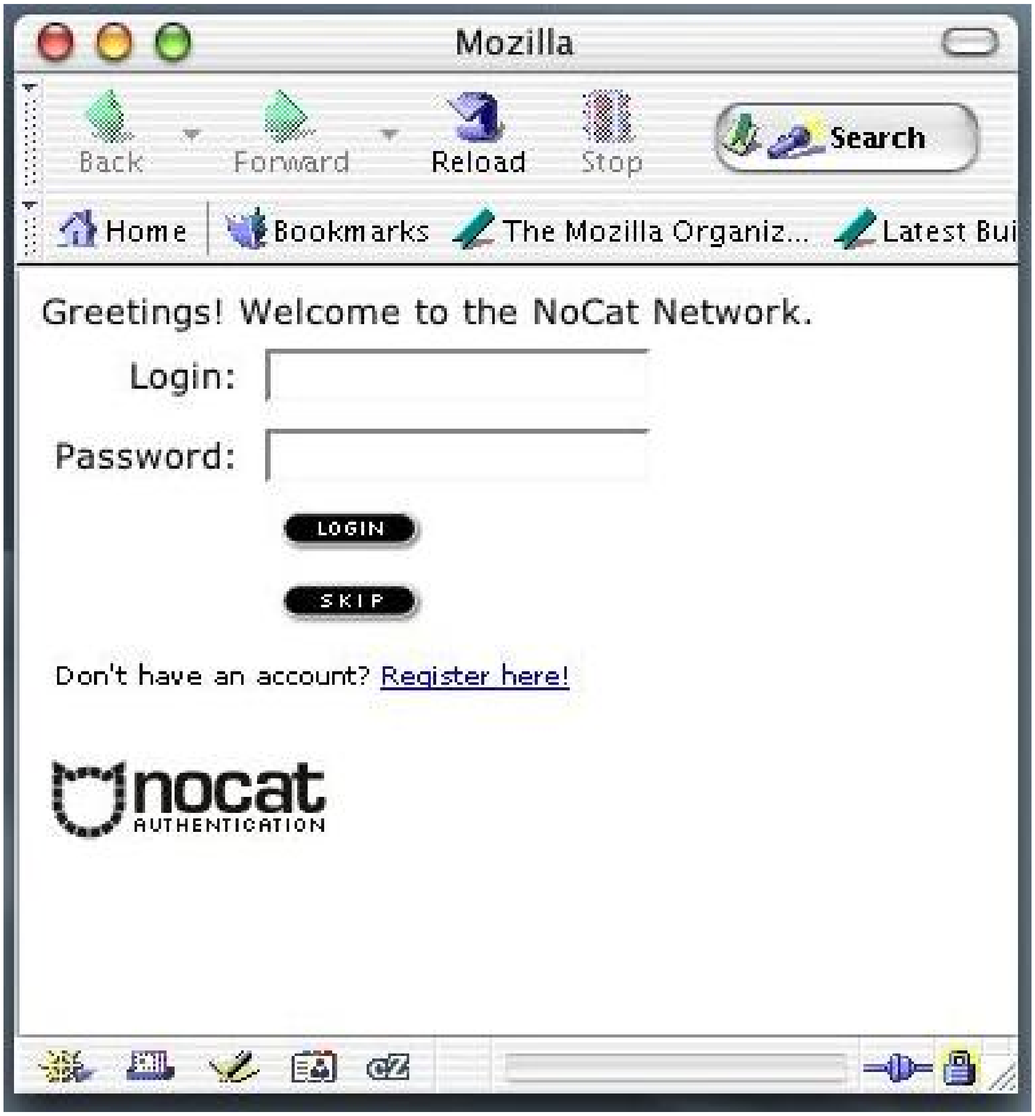
```
bash>ssh zornnh@10.0.1.1
zornnh's Password:

gateway>
```

As long as you stayed logged in, you will have access. Once you log out, access will be taken away.

To use the authentication gateway with NoCatAuth installed, configure your client machine to use DHCP. Install a web browser such as Mozilla. Start up the web browser. The browser should be redirected to the authentication screen.

Figure 1. Nocat Login



Greetings! Welcome to the NoCat Network.

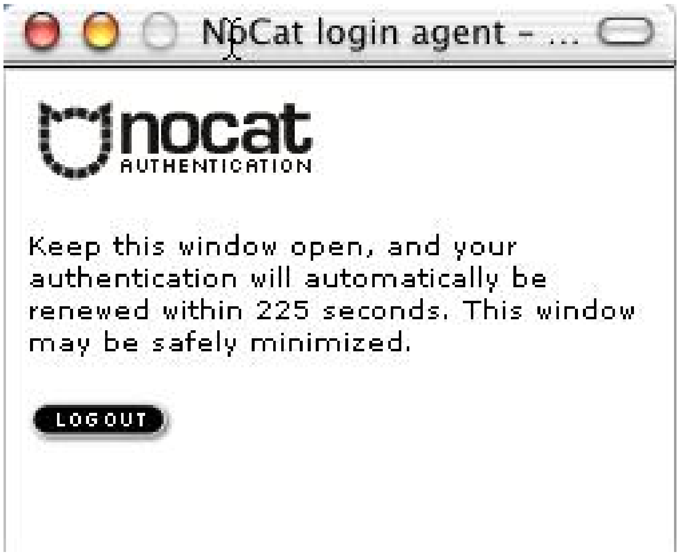
Login:

Password:

Don't have an account? Register here!

Submit your username and password and a screen will pop up explaining that you are authenticated to the network and to keep the window open to remain authenticated. Click logout or close the window to end the session.

Figure 2. Authentication Window



Keep this window open, and your authentication will automatically be renewed within 225 seconds. This window may be safely minimized.

5. Concluding Remarks

- This method of security does not rely on the security provided by the wireless network community. It assumes that the entire wireless network is insecure and outside of your network.
- The gateway does not encrypt traffic. It only allows you access to the network behind it. If encryption and authentication are desired, a VPN should be used.

6. Additional Resources

- A document (http://www.nas.nasa.gov/Groups/Networks/Projects/Wireless/index.html) describing the NASA implementation of the authentication gateway.
- A white paper (http://www.ualberta.ca/~beck/authgw.html) describing how the University of Alberta created an authentication gateway.
- Nocat.net (http://nocat.net) has an authentication gateway for wireless networks. This software has a web based client.
- Horatio: Authenticated Network Access (http://www.cs.utexas.edu/users/mcguire/software/horatio/) is a firewall authentication tool. The premise: Legitimate users want to attach laptops and other mobile hosts to the network, but security demands that illegitimate users be prevented from accessing the internal, secure network and from abusing the general Internet.

7. Questions and Answers

This is just a collection of what I believe are the most common questions people might have. Give me more feedback and I will turn this section into a proper FAQ.

1. Why are the iptables rules not flushing out when a client closes the telnet window? It works if the client logsout of the telnet session. In case of ssh the rules get flushed even if the ssh window is closed.

   I have not come up with a good answer or solution to this problem. Logu has contributed some modifications to pam_iptables and a set of other tools to solve this problem. These tools can be found in the contrib (http://www.itlab.musc.edu/~nathan/pam_iptables/contrib) directory with pam_iptables.

2. What does NoCat not work in IE6? It seems to authenticate but doesn't write the firewal rule.

   Make sure your nocat html contains the following: < meta http-equiv="Refresh" content="$redirect" />

   The html files that should contain this metatag are login_ok.html,renew.html, and renew_pasv.html.