Authentication Gateway HOWTO

Nathan Zorn

zornnh@musc.edu

Revision History

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.

Table of Contents

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

This is the initial release.

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

1.4. Credits

Jamin W. Collins

Kristin E Thomas

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.

2.2. PAM for Netfilter rules.

This is a pluggable authentication module (PAM) written by Nathan Zorn that can be found at http://www.itlab.musc.edu/~nathan/pam_iptables.

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 .

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. 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.

2.5. DNS Server

The gateway box also serves as a DNS server for the public network. I installed 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 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
```

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
```

Once the rules are in place 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
```

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. PAM iptables Module

This module is a PAM session module that inserts the firewall rule needed to allow forwarding for the authenticated client. To set it up simply get the source 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
```

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.

The default interface for pam_iptables is eth0. This default can be changed by adding the interface parameter.

```
session required /lib/security/pam_iptables.so interface=eth1
```

This is only needed if the interface name that connects to the external network is not eth0.

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**.
3. Log out of the box to make sure the rule is removed.

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

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 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] /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
```

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
```

3.5. 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.

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 describing the NASA implementation of the authentication gateway.
- A white paper describing how the University of Alberta created an authentication gateway.
- Nocat.net has an authentication gateway for wireless networks. This software has a web based client.

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.