Configuring NDS LDAP authentication for the Squid Proxy Server
Version 0.1 - Thursday, November 02, 2006
By: Mark Lachniet

Table of Contents

1.0 Overview

This document is intended to provide a simple overview of how to configure a Squid proxy server to authenticate and log user activity. Specifically, this document is geared towards environments with Novell NetWare and SuSE Linux Enterprise server. There are a number of web pages and papers[1][2][3] on the topic of squid LDAP authentication, most of them better than this one, but they do not provide all of the detail in one place. What I describe is not the best way to do this from a security perspective, and it also doesn't scale well (it works for a single user OU) but at least you can get it working and update it later if you wish.

2.0 NDS LDAP Requirements

By default, your NDS servers should support LDAP over SSL. If you need more information on this, please refer to the appropriate Novell documentation, such as the NDS eDirectory Administration Guide[4]. Specifically, you may need to enable SSL support, as per the section entitled Enabling Secure LDAP Connections[5]. Using SSL is not absolutely necessary, but if you don't use it, you'll be sending administrative user credentials across the wire in cleartext, where they could be intercepted by a hacker. In any event, the example configuration files assume you have it working.

[1] http://www.novell.com/coolsolutions/trench/5750.html
[2] http://wiki.squid-cache.org/ConfigExamples/SquidAndWebwasher?highlight=%28ldap%29#head-05d91cde5e0516d2a1e819a766a75a3fd0b95da8
[3] http://www.afp548.com/article.php?story=20041207040115940
[4] http://www.novell.com/documentation/ndsam/taoenu/data/a2iii88.html
[5] http://www.novell.com/documentation/ndsam/taoenu/data/a5bwzv3.html

3.0 NDS User Requirements

You will need to have a user ID with significant rights to your NDS directory. An admin-equivalent user ID will work in this case, but this is probably more access than you need. You should be able to create a user ID and grant them *only* access to LDAP lookups, and not the whole NDS tree, but this is outside of the scope of this document. If you know how to do this, send me an e-mail and I'll include it. For our purposes, I'm assuming you have a user ID with full rights, which is somewhat dangerous, as we'll be putting these credentials into a plaintext configuration file. You might be able to get away with granting read and browse access to the NDS tree to the user account, and possibly administrator rights to the LDAP objects, but I haven't confirmed this.

4.0 Data to Collect Before Starting

Before you begin working, there are a few things you want to write down ahead of time. At a minimum, collect the following pieces of data:

Object	Name	Example	Purpose
Normal NDS Username	<username>	mlachniet	For testing client access
Normal NDS Password	<password>	mlpassword	
LDAP Server IP	<ldapIP>	192.168.2.100	Server running LDAP service
LDAP Server Port	<ldapport>	636	Port the server is listening on
LDAP User ID to connect	<adminusername>	cn=administrator,ou=USERS,o=CUST	Account with rights to query LDAP / NDS
LDAP Password to Connect	<adminpassword>	adminpassword	
LDAP Base DN	<basedn>	ou=USERS,o=CUST	The container where all the users are
Linux Box IP Address	<linuxip>	192.168.2.101	IP Address of the linux box
Linux Box Squid Port	<squidport>	3128	The port that Squid listens on
Linux Box Root Password	<linuxrootpw>	rootpassword	The root password to the Linux box

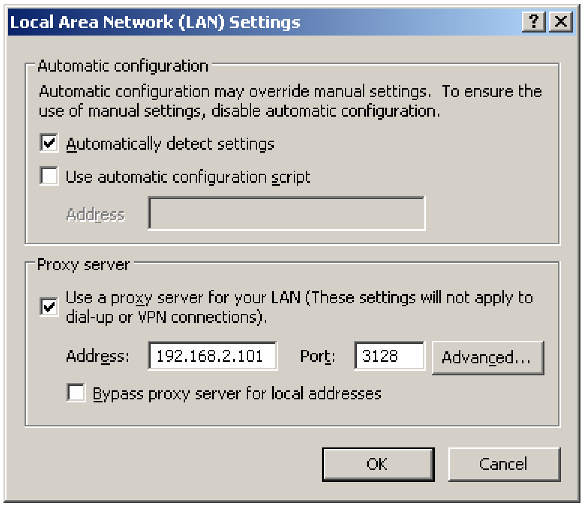
As you can see, we need a couple of user ID's – one for regular client access (for testing) and another that has rights to query NDS. We need to know the server IP addresses, as well as the contexts. Please note that you need to understand your X.500 naming conventions and convert these to LDAP format, but this is well covered in the Novell documentation referenced earlier.

5.0 Configuring Squid

We will now attempt to get Squid working.

5.1 Verifying that Squid Works

Once you have collected your data, log into your Linux server. Verify that squid is running using YaST. If it isn't, start it with YaST or a command such as '*/etc/init.d/squid start*' and verify that you can use it at all. By default you'll configure your test workstation to use the Linux server's IP address, port 3128 as your proxy. This is set in IE from Tools, Internet Options, Connections, LAN Settings, Proxy Server, such as the following:


Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 192.168.2.101 Port: 3128

□ Bypass proxy server for local addresses

Now save your settings. If everything worked, you can now see a web page, which was proxied through Squid. You can also watch the squid logs to verify that things are happening with a command such as '*tail –f /var/log/squid/access.log*'.

If this doesn't work, first verify that Squid is installed and started. Also, if you have the firewall turned on, make sure that there is an exception for Squid (usually on TCP port 3128). You can also test that the port is even open by telnetting to it from a client workstation (e.g. 'telnet 192.168.2.101 3128'.

5.2 Testing LDAP connectivity

Before you even try to get Squid working, you should verify that you can get LDAP lookups working at all. There is more than one LDAP tool on the average SuSE Linux system. In this case, the only one we care about is 'squid_ldap_auth'. Depending on how you installed it, you may find this in /usr/sbin. If you don't know where it is, you can find it with a command such as '*find / -name squid_ldap_auth*'. Once you find it, change to that directory, and test to see if you can query LDAP.

You can issue a command line to bring up the squid_ldap_auth tool. Most of the arguments are obvious. The –f argument, which tells the which attributes to look up, and the –Z argument tells it to use SSL. Other than that, it's pretty straight forward.

An example would be:

```
./squid_ldap_auth -b <basedn> -h <ldapIP> –D <adminusername> -w <adminpassword> –f \
"(&(objectclass=person)(cn=%s))" -Z
```

Or if you used our example values it would be:

```
./squid_ldap_auth -b ou=USERS,o=CUST -h 192.168.2.100 –D \
cn=administrator,ou=USERS,o=CUST -w adminpassword –f \
"(&(objectclass=person)(cn=%s))" -Z
```

IMPORTANT! The above examples are supposed to be all on one line. The backslash character is used in UNIX to indicate that the command is continued on the next line of text.

Now, you will have a cursor sitting on a blank line. This is not an error. Simply type in username of the test user, then a space, then the password and hit enter. If you get an ERR, it means that something is screwed up. If you get an OK, then you are communicating correctly and should be all set.

5.3 LDAP Auth in Squid

Now that we know we can authenticate to NDS from the command line, it's easy to get Squid to use LDAP. You'll need to do two things – set up the authentication program, and then create an ACL that uses it. Open up your squid configuration file using an editor (for example '*pico /etc/squid/squid.conf*' and then add the following text.

1. Find the area below the section with comments starting with '#auth param' and add the following:

```
auth_param basic program ./squid_ldap_auth -b ou=USERS,o=CUST -h 192.168.2.100 \
–D  cn=administrator,ou=USERS,o=CUST -w adminpassword –f \
"(&(objectclass=person)(cn=%s))" -Z

auth_param basic children 50

auth_param basic realm Web-Proxy

auth_param basic credentialsttl 1 minute
```

NOTE: here again, the first line is a long one that wraps over multiple lines in this document! Make sure its all in one line in the configuration document. Replace the values here with your own values.

ADDITIONAL NOTE: Putting your admin password in a text file is dangerous. I strongly recommend you keep this box patched so it doesn't get hacked, and also that you NOT let any non-admin users onto the system. At a minimum, you should lock down the file permissions so users cannot read it.

This section tells squid what program to use to authenticate users. Any program that takes a username and password on STDIN and kicks back an OK or ERR would work here, but we have already verified that we can do this with LDAP.

2. Find the area below the section with comments starting with '#acl' and add the following:

acl password proxy_auth REQUIRED

This sets up an access control list that requires authentication.

3. Find the area below the sections with comments starting with '# http_access'

```
http_access allow password
```

This tells Squid to allow http_access using the acl we previously created.

Now, restart squid using YaST or a command such as '*/etc/init.d/squid restart*' and test it from a browser. If all goes well, you will get a password popup, and you can enter in your test user ID and password to get out to the Internet. You now have squid authentication working, and you have a user ID associated with every access.

6.0 Log Analysis

Although it is outside of the scope of this paper, I strongly recommend you use some kind of log analysis on these log files. That way you can really understand what is going on with your network. One way to do this is to set up an FTP user account with rights to the squid log directory, and then use Sawmill[6] log analysis software to parse the logs. Using sawmill, you can get a handy HTML report of activity sent to you every night, week, month or whatever, as well as having the ability to do ad-hoc reporting. This is a good way to identify your web hogs, as well as inappropriate usage.

7.0 Conclusion

This simple document was intended to give you a quickstart on getting LDAP authentication working on SuSE in a Netware / LDAP environment. If you have any suggestions for improvement, please send them to me at mark@lachniet.com.

Thanks,

Mark Lachniet

[6] http://www.sawmill.net