

Squid With LDAP Authentication

Author : Gopal Singh Bhandari

Categories : [Ldap Server](#), [Uncategorized](#)

Date : Jun 6, 2015



- [Facebook](#)

- [Twitter](#)

- [Google+](#)

- [Gmail](#)

Linux Gateway

Linux Tutorials, Guides & Resources
<http://linuxgateway.in>



www.openpath.in

Want to Become a
Linux Professional...???

Join



Call us : 9810179147 or write us : vikas@openpath.in



 KV IT

Linux Solutions

- ❖ Mail/Proxy Server
- ❖ Firewall Solutions
- ❖ Migration from other OS
- ❖ LDAP Server
- ❖ SAMBA Server



www.linuxsolutions.org.in

Squid Proxy Configuration

SQUID proxy servers works between a local network and Internet. Requests from local clients for web services can be handled by the proxy server. it can often give your users the data they need without their systems having to look to the Internet. Squid proxy filter everything from porn site to advertise , videos.

In our example we will not go to deep about squid server for detail about squid server [Click Here](#) , here we will configure squid server authenticate by LDAP User Accounts.

Note: Tested on centos 6.5 64bit

Set date and time on both server (ldap server and porxy server)

=====
ldap server ip address: 192.168.0.157 ([Check LDAP Configuration](#))

proxy server ip address: 192.168.0.202
=====

Login your proxy server

Note: ldap server should be ping and hostname should be resolved from proxy server

```
#vim /etc/hosts
192.168.0.157 ldap.example.com
```

```
#yum install squid
```

Now Install The LDAP Squid Module

```
#yum install nss-pam-ldapd
```

Now take the backup of your squid.conf file

```
#cp /etc/squid/squid.conf /etc/squid/squid.conf.org
```

Now open the squid.conf file and edit

```
#vim /etc/squid/squid.conf
```

```
auth_param basic program /usr/lib64/squid/squid_ldap_auth -b
“dc=example,dc=com” -f “uid=%s” -h 192.168.0.157
# Recommended minimum configuration:
#
acl manager proto cache_object
acl localhost src 127.0.0.1/32 ::1
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32 ::1
```

```
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
#acl localnet src 10.0.0.0/8 # RFC1918 possible internal network
#acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
#acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
acl trusted_user proxy_auth "/etc/squid/trusted_user"
acl blocksites dstdomain "/etc/squid/blocksites"
#
# Recommended minimum Access Permission configuration:
#
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager
# Deny requests to certain unsafe ports
http_access deny !Safe_ports
# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports
# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet
#http_access allow localhost
http_access allow trusted_user !blocksites
# And finally deny all other access to this proxy
```

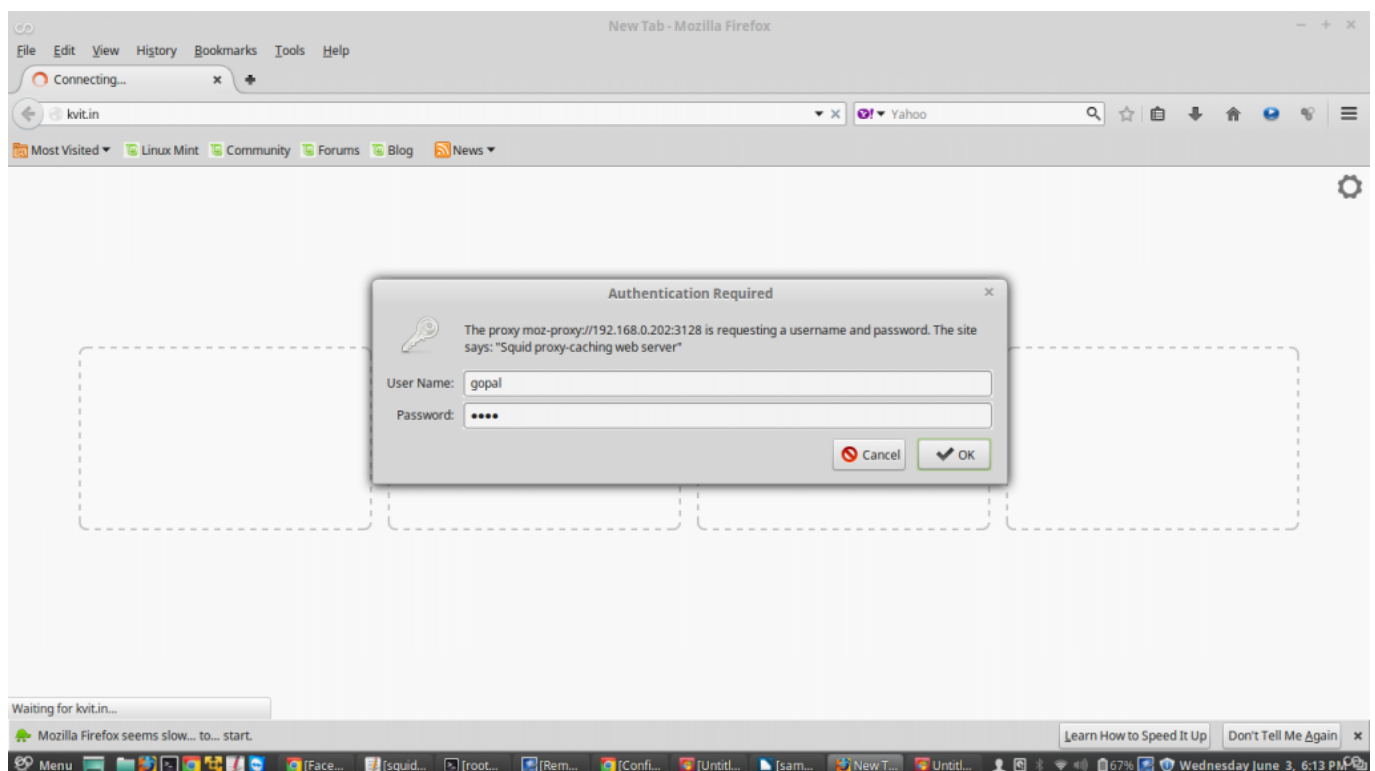
```
http_access deny all
# Squid normally listens to port 3128
http_port 3128
visible_hostname = JPSGN
# We recommend you to use at least the following line.
hierarchy_stoplist cgi-bin ?
# Uncomment and adjust the following to add a disk cache directory.
#cache_dir ufs /var/spool/squid 100 16 256
# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid
# Add any of your own refresh_pattern entries above these.
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
refresh_pattern . 0 20% 4320

:wq
```

Here trusted_user acl hold the list of valid users who already created on ldap sever using LAM

blocksites acl hold the list of sites we want to deny on my network and users.

Now open the browser and set the proxy setting and give the user name or password of your ldap account.



Enjoy.....!!!!!!!



[Gopal Singh Bhandari](#)

Linux Engineer At
KV IT-Solutions Pvt. Ltd.



- [Facebook](#)

- [Twitter](#)

- [Google+](#)

- [Gmail](#)