Installing Squid with Active Directory Authentication

18May06

Proxy servers are fairly essential devices that should be part of a network's perimeter defense strategy. They are devices that allow clients to indirectly access network services via a connection through them. In an enterprise environment, proxy servers are used to aid in enforcement of acceptable use and security policies.

There are a number of reasons for using a proxy server as part of securing a network but that is beyond the scope of this document.

The 10 Legged Creature.

One of the premier proxy servers available today is Squid. It is the most popular HTTP proxy available today, mainly because it is offers a comprehensive set of features, is highly configurable all while being open source and free. It runs on just about any Linux distribution and scales better than any other application of its kind.

For the sake of this exercise, Squid is being deployed to an enterprise network to act in the capacity of a web proxy. By doing so, Squid will be an intermediary for all web browsing between network users and the destinations web sites they desire to browse. When a user requests to visit a site that request will go first to Squid, which will then establish a connection with the destination, transfer the data from the web site to its cache and then pass that data back to the requesting user.

In many instances Squid will even pass the data from its local cache back to the users, both saving time and precious bandwidth. Depending on which algorithm is selected when configuring Squid will determine how Squid decides whether or not to serve the local cache to a user or whether to fetch new data.

Mayday, Mayday!

When I set out to install Squid so that it could perform active directory authentication I was unable to locate any single resource that could explain, in detail, the steps required in order to make this happen. What I did find, however, was a variety of instructions related to various aspects of the entire process. The sum of all the information that I discovered is contained in this document, which will hopefully serve as a means of helping someone else achieve the same goal I was aiming for.

The following are the instructions for installing Squid Proxy Server so that it performs Active Directory authentication off of a Windows 2003 domain controller. Squid is configured so that the browsers must explicitly point to it, which means that it is not being setup to function as a transparent proxy. This entire design was performed on a Dell 1650 running Gentoo Linux 2006.0.

Although the act of downloading, compiling and installing applications on a Gentoo box is slightly different than that of an RPM based distribution (like Red Hat) the same basic configuration directions are applicable. The key difference is Gentoo's USE flag convention

whereas the other distributions will force the use of compile time options (i.e. using "–with-winbind" when running configure, as an example).

The following software is necessary in order to make all of this work as planned.

- Squid Proxy Server
- SAMBA
- OpenLDAP
- MIT Kerberos

Installation of this software on Gentoo is rather easy however there is a USE flag caveat. In order to ensure that the software is compiled with the necessary options to make this all work properly specific Gentoo USE flags need to be set. This can be done on the command-line while emerging the software or by modifying the make.conf file. Whichever method is selected, the following USE flags need to be set:

```
USE="kerberos ldap pam"
```

Using the command-line, emerge the software as follows:

```
USE="kerberos ldap pam" emerge squid samba openldap mit-krb5
```

If make.conf was updated to reflect the necessary USE flags then do the following:

```
emerge squid samba openldap mit-krb5
```

Once emerge is done working the lovely magic it performs it will be time to modify the various configuration files.

Squid

This is only the applicable portion of the squid.conf file required for active directory authentication. In the event that a complete squid.conf file is necessary then take a look here.

```
/etc/squid/squid.conf

# Active Directory configuration
auth_param ntlm program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-
ntlmssp
auth_param ntlm children 30
auth_param ntlm max_challenge_reuses 0
auth_param ntlm max_challenge_lifetime 2 minutes
auth_param ntlm use_ntlm_negotiate on

auth_param basic program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-
basic
auth_param basic children 5
auth_param basic realm Squid Proxy Server
auth_param basic credentialsttl 2 hours

# Only allow authenticated users to use the proxy
# Add these in the appropriate places in squid.conf
acl authenticated_users proxy_auth REQUIRED
```

```
...
http_access allow authenticated_users
```

SAMBA

/etc/samba/smb.conf

```
[global]
netbios name = proxyserver
realm = DOMAIN.COM
workgroup = DOMAIN
security = ADS
password server = dc01.domain.com dc02.domain.com dc03.domain.com
socket options = TCP_NODELAY SO_RCVBUF=16384 SO_SNDBUF=16384
idmap uid = 10000-20000
winbind enum users = yes
winbind uid = 10000-20000
winbind gid = 10000-20000
winbind separator = +
winbind use default domain = yes
encrypt passwords = yes
log level = 3 passdb:5 auth:10 winbind:5
```

Kerberos

/etc/krb5.conf

```
[libdefaults]
        ticket_lifetime = 600
        default_realm = DOMAIN.COM
        default_tkt_enctypes = des3-hmac-sha1 des-cbc-crc
        default_tgs_enctypes = des3-hmac-sha1 des-cbc-crc
        dns_lookup_realm = false
        dns_lookup_kdc = false

[realms]
        DOMAIN.COM = {
                kdc = dc01.domain.com:88
                kdc = dc02.domain.com:88
                kdc = dc03.domain.com:88
                admin_server = dc01.domain.com:749
                default_domain = DOMAIN.COM
        }

[domain_realm]
        .domain.com = dc01.domain.com
        domain.com = dc01.domain.com

[kdc]
        profile = /etc/krb5kdc/kdc.conf

[logging]
        kdc = FILE:/var/log/krb5kdc.log
        admin_server = FILE:/var/log/kadmin.log
        default = FILE:/var/log/krb5lib.log
```

PAM

```
/etc/pam.d/samba

auth    required  pam_nologin.so
auth    required  pam_stack.so service=system-auth-winbind
account  required  pam_stack.so service=system-auth-winbind
session  required  pam_stack.so service=system-auth-winbind
password  required  pam_stack.so service=system-auth-winbind

/etc/pam.d/squid

auth    required  /lib/security/pam_stack.so service=system-auth-winbind
account  required  /lib/security/pam_stack.so service=system-auth-winbind

/etc/pam.d/system-auth

auth    required  pam_env.so
auth    sufficient  pam_unix.so likeauth nullok
auth    required  pam_deny.so

account  required  pam_unix.so

password  required  pam_cracklib.so difok=2 minlen=8 dcredit=2 ocredit=2
retry=3
password  sufficient  pam_unix.so nullok md5 shadow use_authtok
password  required  pam_deny.so

session  required  pam_limits.so
session  required  pam_unix.so
```

Once all the aforementioned software has been configured as depicted the proxy server needs to be added to the Windows 2003 domain. This is necessary so that the proxy server can perform authentication in conjunction with a Windows 2003 active directory domain controller.

To join the Linux machine to a Windows 2003 domain perform the following:

```
sudo net ads join Servers/Linux -U AdminAcct -S dc01.domain.com
```

If everything went as planned then a message will be echoed on the screen depicting as such. After a few moments, once the domain controllers replicate, the proxy server should show up in the OU that was specified when joining the domain. In the example above, the Linux server proxyserver.domain.com would show up in the Linux OU, under the Servers OU in the Windows 2003 domain named domain.com.

In the event that an error occurred while joining the domain check syslog for possible errors.

At this point, start SAMBA and winbindd by performing the following:

```
/etc/init.d/samba start
/usr/sbin/winbindd
```

Both of these are necessary in order for Squid to be able to properly perform active directory based authentication. Ensure that winbindd is functioning properly by issuing the following command. If all goes as planned then the following will be the response:

```
proxyserver ~ # wbinfo -t
checking the trust secret via RPC calls succeeded
```

Ensure that Squid is able to properly perform active directory authentication by testing the helper application:

```
/usr/bin/ntlm_auth --helper-protocol=squid-2.5-basic
DOMAIN+username password
utils/ntlm_auth.c:check_plaintext_auth(292)
  NT_STATUS_OK: Success (0×0)
```

Assuming that everything has gone as listed above, start up Squid by issuing the following:

```
/etc/init.d/squid start
```

Configure a web browser, such as Firefox or Internet Explorer, to point directly to the proxy server and ensure that browsing is possible without ever being offered an authentication dialogue box. This is testing to ensure that NTLM authentication with the Windows 2003 active directory domain controller is working properly. Confirm that traffic is being properly authorized by tailing the Squid access log file.

```
tail -f /var/log/squid/access.log

1147739650.906   9969 192.168.1.203 TCP_MISS/200 4244 CONNECT
mail.google.com:443 DOMAIN+username DIRECT/64.233.185.19 -
1147739672.965   1085 192.168.1.203 TCP_REFRESH_MISS/200 2321 GET
http://www.cnn.com/.element/ssi/auto/1.4/pipeline_mp/live.mhtml?
DOMAIN+username DIRECT/64.236.29.120 text/html
1147739673.871    907 192.168.1.203 TCP_MISS/200 3027 GET
http://i.cnn.net/cnn/.element/img/1.3/pipeline/keyframes/88×49/stream1.jpg?
DOMAIN+username DIRECT/64.236.24.136 image/jpeg
1147739683.229      0 192.168.1.203 TCP_DENIED/407 1745 CONNECT
mail.google.com:443 - NONE/- text/html
1147739683.243      0 192.168.1.203 TCP_DENIED/407 1874 CONNECT
mail.google.com:443 - NONE/- text/html
1147739693.881  10636 192.168.1.203 TCP_MISS/200 4340 CONNECT
mail.google.com:443 DOMAIN+username DIRECT/64.233.185.83 -
```

When using NTLM authentication it is normal to see two simultaneous TCP_DENIED/407 errors. This is due to the nature of the challenge/response mechanism of NTLM authentication.

In the event that no username appear in the squid access log, or password dialogue boxes appear, then check the squid.conf file to ensure that the ACL's are setup properly. Also ensure that winbindd is functioning, as depicted above. If changes are made to the squid.conf file then squid needs to be restarted in order for those modifications to take affect.

If everything is working as planned then ensure that Squid and SAMBA start automatically upon reboot by issuing the following:

```
rc-update add squid default
rc-update add samba default
```

Modify the following file so that winbindd is started after a reboot:

```
/etc/conf.d/local.start

# Start the winbind daemon so we can do AD lookups in Squid
/usr/sbin/winbindd
```

Squid is now properly configured to perform Windows 2003 active directory authentication. Enjoy the added security benefit that a proxy server solution offers, especially since it can perform authentication.

The following resources were used in both the configuring of Squid with active directory authentication, as well as putting this document together:

1. http://www.squid-cache.org/Doc/FAQ/FAQ_long.html#winbind
2. http://info.ccone.at/INFO/Samba-2.2.12/winbindd.8.html
3. http://acd.ucar.edu/~fredrick/linux/samba3/
4. http://gentoo-wiki.com/HOWTO_Adding_a_Samba_Server_into_an_existing_AD_Domain

http://cryptoresync.com/2006/05/18/installing-squid-with-active-directory-authentication/