SCUOLA D'ARTI E MESTIERI	**Informatica modulo 300** Integrare in una rete servizi di più piattaforme	06.02.2015
CLASSE **4**	Proxy SQUID, autenticazione	Pratica

Introduzione

In ambiente linux Squid è sicuramente il server proxy più utilizzato, che si integra perfettamente con i firewalls IPTables, Monowall, IPCop ecc.

Per permettere di dare un accesso controllato agli utenti di una rete, Squid può essere configurato per utilizzare diversi tipi di autenticazione.

In questo caso parliamo solo dell'autorizzazione ad accedere e non di monitoraggio, questo può sempre essere attivato ma l'interpretazione sarà poi affidata ad altre applicazioni che permettono la presentazione dei risultati e delle statistiche.

Possiamo suddividere la gestione dell'autorizzazione all'accesso ad Internet in due grandi categorie:

1. autorizzazione tramite utenti gestiti internamente a Squid
2. autorizzazione tramite un servizio amministrativo centrale tipo LDAP o MS-Active Directory

In questo documento di occuperemo solo della gestione dei casi del secondo tipo, ricordando che comunque anche MS-Active Directory si basa sulle specifiche di base di LDAP.

Per la gestione delle autorizzazioni tramite MS_Active Directory, SQUID ha bisogno di librerie esterne che saranno configurate ed utilizzate tramite le ACL di SQUID.

Fondamentalmente abbiamo le seguenti possibilità:

1. Controllo d'accesso tramite autenticazione di tipo Basic:
   si tratta del sistema più semplice, permette l'autenticazione verso un server Active Directory. La password è trasmessa in chiaro se non si usa una connessione SSL. In questo caso però, tutti i dati saranno criptati e quindi l'efficienza del sistema viene ridotta.
   Funzione implementata a partire dalla versione SQUID 2.5 compilata con LDAP helpers.
   Per questo tipo di autenticazione il server SQUID NON deve essere necessariamente in dominio.

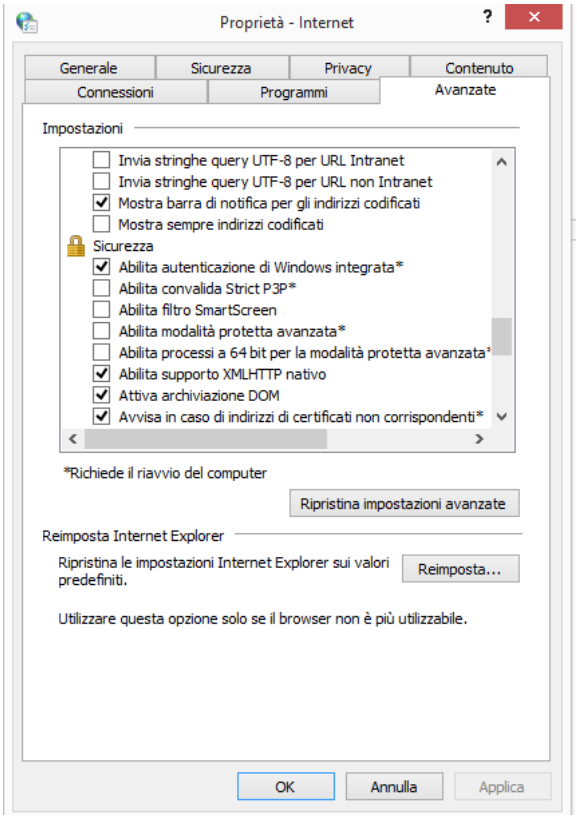
2. Controllo d'accesso tramite autenticazione di tipo NTLM Integrated:
   si tratta del sistema di autenticazione con password criptata introdotta a partire da Windows server NT4.0 SP4 e successivamente e successive. Risulta abbastanza sicura ma usa il Controllo di Ridondanza Ciclico (CRC) o l'algoritmo di classificazione dei messaggi (RFC 1321) con criptazione RC4.
   Funzione implementata a partire dalla versione SQUID 2.6.
   Il server SQUID DEVE appartenere al dominio.

3. Controllo d'accesso tramite autenticazione Kerberos:
   si tratta del sistema più sicuro, implementata a partire dalla versione Windows server 2000, utilizza il sistema di criptazione AES.
   È un sistema sicuro, con dati criptati, implementata in modo efficace con due helpers a partire dalla versione SQUID 2.7.
   Il server SQUID DEVE appartenere al dominio.

Attenzione, la scelta del sistema di autenticazione dipende dal server che gestisce Active Directory ma anche dal tipo di sistema operativo client e dalla versione del Browser.

Prima di decidere quale utilizzare, assicurarsi che nel parco macchine non ci siano macchine clients e/o browser obsoleti. In questo caso controllare che ci sia la possibilità di effettuare un aggiornamento.

Di seguito vedremo l'esempio di configurazione per i tre tipi di controllo d'accesso, Kerberus, NTLM e Basic.
Questo tipo di autenticazione offre la possibilità di autenticarsi solo una volta (Single Sign ON) e di non richiedere l'autenticazione per ogni oggetto presente in una pagina web che costruisce una connessione.
Se però una macchina nel sistema non è grado di gestire l'autenticazione con Kerberus, Squid deve poter "abbassarsi" e richiedere un'autenticazione di tipo NTLM integrated o addirittura Basic.



Prerequisiti:

I clients windows devono avere abilitata la voce "Abilita autenticazione di Windows integrata" nelle opzioni Internet -> Avanzate

Configurazione DNS:

Nel server DNS di MS-AD server aggiungere un record A per il nome del server proxy ed assicurarsi che il rispettivo PTR (reverse DNS) sia stato creato e funzioni.

(Controllare con nslookup nome_proxy, il contrario con nslookup ip_proxy)

Controllare che il proxy usi il server DNS di MS-AD per la risoluzione dei nomi aggiornando il contenuto del file `/etc/resolv.conf`.

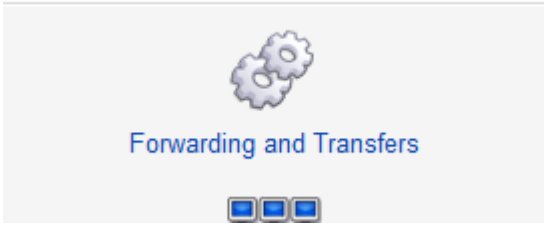
Modificare nel server DNS del Controllore di dominio l'indirizzo Forwarders in m odo che non punti più sul server DNS del CPT ma su quello del proxy.

a) In poche parole, tutte le macchine, compreso il proxy si rivolgono al server DNS del controllore di dominio.
b) Se questi non è in grado di rispondere alla richiesta, si rivolge al server DNS del proxy tramite una richiesta di forwarding.
c) Quest'ultimo non fa che inoltrare tale richiesta al server che trova nella sua configurazione di forwarding e cioè al server DNS del CPT.

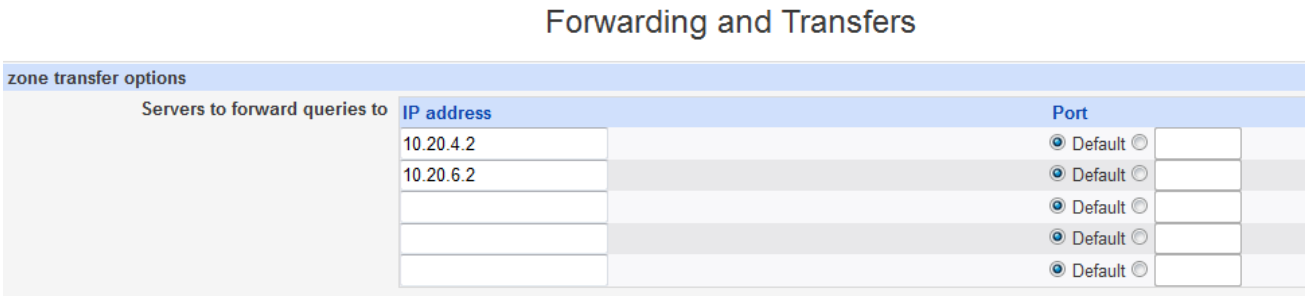
Squid deve poter fare da forwarders per le richieste che arrivano dall'interno per fare questo, bisogna installare sulla macchina che ospita squid un server DNS che svolga unicamente la funzione d'inoltro.

Tramite Webmin, installare sulla macchina proxy il server **BIND9**
In seguito, dal menu server -> BIND DNS Server, configurare:

a) Forwarding and transfer

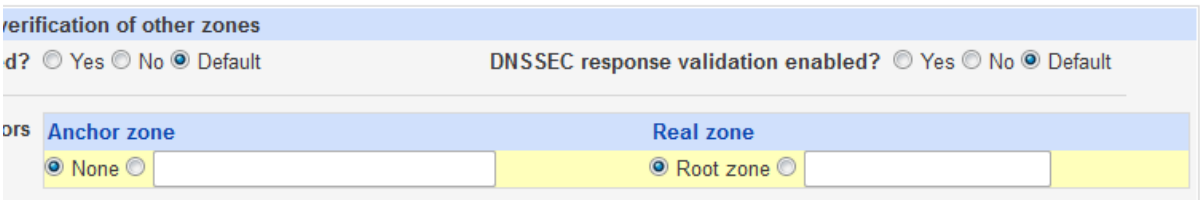


inserire solo gli indirizzi dei DNS del CPT:



b) Controllare che le impostazioni di DNSSEC Verification sia impostata su Default

Se non lo fosse, impostarla su default oppure su NO:



c) Applicare le configurazioni

Se invece di utilizzare webmin si volesse configurare BIND tramite il file di configurazione, editare il file /etc/bind/named.conf.options:

```
sudo nano /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };
```

Aggiungere

```
        auth-nxdomain no;
        forwarders {
                10.20.4.2;
                10.20.6.2;
                };
};
```

Salvare e riavviare il servizio DNS

Installazione e configurazione del client NTP

Affinché la macchina proxy possa lavorare con il controllore di dominio, è importante che il clock sia sincronizzato, per questo utilizzeremo il servizio NTPD.
Il controllore di dominio, per default ha attivato un server NTP.
Sulla macchina proxy dovremo quindi installare il servizio che vada poi ad effettuare la sincronizzazione.

```
sudo apt.get install ntp
```

In seguito, editare il file /etc/ntp.conf ed inserire il nome del server con il quale sincronizzare l'orologio:

```
sudo nano /etc/npt.conf

# You do need to talk to an NTP server or two (or three).
#server ntp.your-provider.example
server Vostro-ms-ad-server.greenpower.local
```

Installare e configurare Kerberos:

Sulla macchina SQUID installare i pacchetti `krb5-user libkrb53`

`apt-get update`
`apt-get install krb5-user,libkrb53 (libkrb5-3` se avete una versione di Ubuntu uguale o maggiore della 14:04`)`

Nelle finestre di dialogo accettare i valori di default perché in seguito modificheremo il contenuto del file di configurazione ktb5.conf.

Sudo nano /etc/krb5.conf

Rimpiazzare il contenuto con il seguente:

```
[libdefaults]
    default_realm = GREENPOWER.LOCAL
    dns_lookup_kdc = no
    dns_lookup_realm = no
    ticket_lifetime = 24h
    default_keytab_name = /etc/squid3/PROXY.keytab


; for Windows 2008 with AES
  default_tgs_enctypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-md5
  default_tkt_enctypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-md5
  permitted_enctypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-md5

[realms]
    GREENPOWER.LOCAL = {
        kdc = nome-del-server-ms-ad.greenpower.local
        admin_server = nome-del-server-ms-ad.greenpower.local
        default_domain = greenpower.local
    }

[domain_realm]
    .greenpower.local = GREENPOWER.LOCAL
    greenpower.local = GREENPOWER.LOCAL
```

Importante: Se avete un solo Controllore di dominio (DC) rimuovete le voci supplementary di `kdc` dalla sezione `[realms]`, in caso contrario, aggiungete ogni altro DC supplementare.

A dipendenza del tipo di sistema operativo del vostro controllore di dominio, eliminate i commenti della rispettiva parte e commentate quelli che non vi riguardano.

Attenzione: Si dovrebbe utilizzare "Windows 2008 with AES" se possibile. Questo non solo per ragioni di sicurezza ma anche per evitare problemi nell'utilizzazione del nome DNS del server squid al posto del suo indirizzo IP nella configurazione dei browsers.

Esempio di un messaggio d'errore relativo a questo problema:

```
ERROR: Negotiate Authentication validating user. Error returned
'BH gss_accept_sec_context() failed: Unspecified GSS failure.
Minor code may provide more information.'
```

Installazione dei tools per LDAP:
Per poter utilizzare le librerie di LDAp, bisogna installare i relativi tools:

```
apt-get install ldap-utils
```

Autenticazione:
Il proxy utilizza 3 metodi di autenticazione, negoziando dal più alto al più basso in termini di sicurezza, Negotiate/Kerberos -> Negotiate/NTLM, NTLM e -> basic authentication.

Alcune applicazioni non sono in grado di utilizzare Kerberos e devono appoggiarsi su NTLM (esempio: iTunes). L'ordine nel quale sono definiti gli helpers di autenticazione è importante, per esempio, se si desidera utilizzare il broweser iE in un client che non è in dominio.
Se non fosse in grado di negoziare un'autenticazione in Kerberos, potrebbe non riuscire ad abbassarsi al livello NTLM o Basic. In questo caso l'utente continuerebbe a ricevere all'infinito una richiesta di autenticazione.

Kerberos:
Kerberos utilizza il tool mskkutil per gestire le chiavi di Active Directory che però necessita di alcuni pacchetti ausiliari:

```
apt-get install libsasl2-modules-gssapi-mit libsasl2-modules
Attenzione, nel nome l2 non è la cifra dodici ma elle2!
```

in seguito installare il pacchetto msktutil:

a) Se avete avete una versione di ubuntu antecedente la 14.04 utilizzate wget perché msktutil non era inserito nei repository.:

   SYSARCHIT è da sostituire con i386 se avete un sistema a 32 bits o con amd64 se avete un sistema a 64 bits
   La prossima riga va scritta tutta su una linea:

```
wget -O /var/cache/apt/archives/msktutil_0.4-2_SYSARCHIT.deb
"http://fuhm.net/software/msktutil/releases/msktutil_0.4-2_SYSARCHIT.deb"
--no-check-certificate

dpkg -i /var/cache/apt/archives/msktutil_0.4-2_SYSARCHIT.deb
```

   Se alla fine doveste ottenere un errore di dipendenze (mancanza del pacchetto libkbr53, terminare l'operazione con:

   `apt-get install -f` in modo da completare l'installazione con il pacchetto mancante.

b) Se la versione di Ubuntu è uguale o maggiore alla 14.04, allora potete utilizzare l'istallazione tramite apt

```
apt-get install msktutil
```

Ora bisogna generare una chiave per un ticket per Kerberos:
Iniziate una sessione Kerberos verso il server di active directoriy con l'utente amministratore di dominio per aggiungere gli oggetti ad Active Directory

```
kinit administrator

Password for administrator@GREENPOWER.LOCAL
```

Il commando dovrebbe terminare senza errori.
Per controllare se effettivamente è stato rilasciato un ticket si può utilizzare il comando:

```
klist
```

Che ritornerà la descrizione del ticket:

```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@GREENPOWER.LOCAL
Valid starting     Expires            Service principal
01/09/12 09:01:49  01/09/12 19:01:53  krbtgt/EXAMPLE.LOCAL@EXAMPLE.LOCAL
renew until 01/10/12 09:01:49
```

Ora bisogna configurare l'account Kerberos del proxy nel servizio Active Directory tramite il commando msktutil.
Attenzione!!
Per poter utilizzare questo comando, bisogna assolutamente rispettare questi due principi:

1) --computer-name non può essere più lungo di 15 caratteri a causa delle limitazioni di NetBios

2) –computer-name deve essere differente dall'hostname del proxy in modo che l'aggiornamento della password per l'account computer di Kerberos non interferisca con NTLM.

```
msktutil -c -b "CN=COMPUTERS" -s HTTP/lx-proxy-01.greenpower.local -k
/etc/squid3/PROXY.keytab --computer-name LX-PROXY-01-K --upn  \ HTTP/lx-proxy-
01.greenpower.local --server nome-del-server-ms-ad.greenpower.local --verbose
```

Sostituire *lx-proxy-01* e *nome-del-server-ms-ad* con i rispettivi nomi del proxy e del controllore di dominio.

Per una versione di MS-Server 2008 o maggiori, aggiungere –enctypes 28 alla fine:

~~msktutil -c -b "CN=COMPUTERS" -s HTTP/lx-proxy-01.greenpower.local -k /etc/squid3/PROXY.keytab --computer-name LX-PROXY-01-K --upn \ HTTP/lx-proxy-01.greenpower.local --server dc1.greenpower.local --verbose --enctypes 28~~

```
msktutil --auto-update --verbose --computer-name LX-PROXY-01-K --server nome-del-
server-ms-ad.greenpower.local -s HTTP/lx-proxy-01.greenpower.local -k
/etc/squid3/PROXY.keytab
```

Controllare che non ci siano annunci d'errore nella lista d'esecuzione del comando.

Ora bisogna modificare i permessi al file PROXY.keytab appena generato in modo che squid lo possa leggere:

```
chgrp proxy /etc/squid3/PROXY.keytab
```

```
chmod g+r /etc/squid3/PROXY.keytab
```

Alla fine si possono eliminare le credenziali dell'amministratore utilizzate per creare l'account:

```
kdestroy
```

Nel server MS-AD, resettare l'Account Computer in Active Directory selezionando il NOME-PROXY-K con il tasto destro del mouse, scegliendo "Reset Account" in seguito eseguire msktutil come segue per essere certi che il keytab sia aggiornato in modo corretto e che lo stesso sia originato com msktutil dal file /etc/krb5.conf correttamente:

```
msktutil --auto-update --verbose --computer-name lx-proxy-01-k
```

Nota: anche se nell'inserimento del proxy in Ad il nome deve essere scritto in maiuscolo, la funzione `--auto-update` richiede che il nome `--computer-name` sia scritto in minuscolo.

Se il keytab non dovesse essere trovato, provate ad aggiungere `-k /etc/squid3/PROXY.keytab` al comando per vedere se funziona ed in seguito cercate di trovare l'errore.

Ora bisogna configurare cron in modo che aggiorni automaticamente l'account del computer in Active Directory quando questo scade (tipicamente ogni 30 giorni)
Le variabili SHELL e PATH sono da modificare solo se sapete quello che state facendo.

```
crontab -e
```

Se compaiono delle opzioni di scelta dell'editor, selezionare nano come editor ed inserite la linea seguente:

```
00 4 * * * msktutil --auto-update --verbose --computer-name lx-proxy-01-k|logger
-t msktutil
```

In seguito aggiungere la configurazione seguente a /etc/default/squid3 in modo che squid sappia dove trovare il keytab di Kerberos.

```
nano /etc/default/squid3

KRB5_KTNAME=/etc/squid3/PROXY.keytab
export KRB5_KTNAME
```

Fine della configurazione dell'autenticazione tramite Kerberos

NTLM:
installare Samba e winbind:

```
apt-get install samba winbind samba-common-bin
```

fermare i servizi Samba e Winbind:

```
invoke-rc.d winbind stop && invoke-rc.d smbd stop
```

copiate il file di default smb.conf per conservarlo ed editate un nuovo file smb.conf

```
cp /etc/samba/smb.conf /etc/samba/smb.conf.default
nano /etc/samba/smb.conf

local master = no
workgroup = GREENPOWER
security = ads
realm = GREENPOWER.LOCAL

winbind uid = 10000-20000
winbind gid = 10000-20000
winbind use default domain = yes
winbind enum users = yes
winbind enum groups = yes

load printers = no
printing = bsd
printcap name = /dev/null
disable spoolss = yes
```

Ora possiamo aggiungere il proxy al dominio, ecco perché abbiamo dovuto modificare. Aggiungendogli una k il nome del proxy. Per evitare che il nome del computer accoun NTLM sovrascrivesse quello già generato con Kerberos.

```
net ads join -U Administrator
Enter Administrator's password:
Using short domain name - GREENPOWER
Joined 'LX-PROXY-01' to realm 'greenpower.local'
```

Ora possiamo rilanciare Winbind e Samba e controllare l'accesso al domino:

```
invoke-rc.d smbd start && invoke-rc.d winbind start
```

Se ci fossero dei problemi con questo commando, utilizzare:
```
/etc/init.d/smbd start
/etc/init.d/winbind start
```

Poi effettuare il controllo d'accesso al dominio con un utente di test già esistente in AD:

```
wbinfo -t
checking the trust secret for domain GREENPOWER via RPC calls succeeded
```

```
wbinfo -a GREENPOWER\\nomeutente%'password'
```
(usare un utente configurator in AD)
```
plaintext password authentication succeeded
challenge/response password authentication succeeded
```
Ora configuriamo i permessi in modo che l'account utente proxy possa leggere il file /var/run/samba/winbindd_privileged:

```
gpasswd -a proxy winbindd_priv
```

Ed ora, come già fatto con Kerberos, aggiungere a cron il comando per modificare la password del computer dinamicamente.

```
crontab -e
05  4  *   *   *     net rpc changetrustpw -d 1 | logger -t changetrustpw
```

Fine dell'autenticazione NTML

BASIC:
Per poter utilizzare l'autenticazione Basic tramite LDAP dobbiamo creare un account per mezzo del quale accedere ad Active Directory.

- In Active Directory definite un utente che si chiami "Squid Proxy" con il nome di account squid@greenpower.local
- Definite la password a vostro piacere.

  Assicuratevi che le condizioni seguenti siano realizzate:
  - Modifica della password al prossimo accesso -> **disabilitato**
  - L'utente non può modificare la password -> **abilitato**
  - La password non scade mai -> **abilitato**
  - L'account è disabilitato -> **disabilitato**

Create ora nel proxy un file per la password utilizzata dall'utente squid in modo che LDAP possa accedere ed avere i permessi necessari: (sostituite squidpass con la password definita precedentemente)

```
nano /etc/squid3/ldappass.txt
```

```
squidpass
```

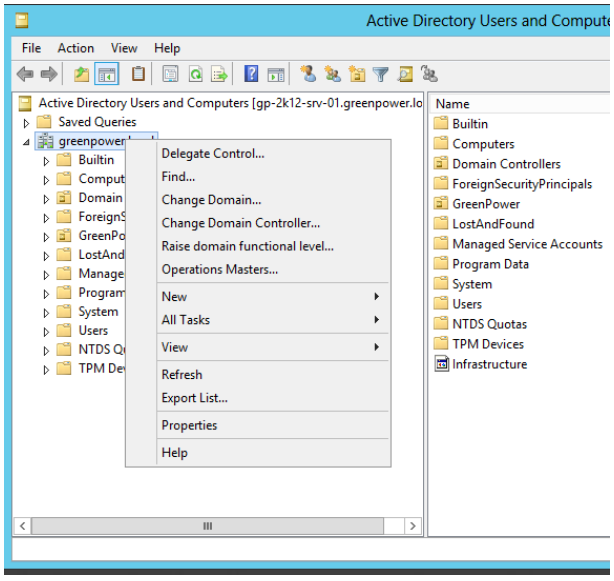
In seguito modifichiamo i permessi d'accesso al file /etc/squid3/ldappass.txt

```
chmod o-r /etc/squid3/ldappass.txt
chgrp proxy /etc/squid3/ldappass.txt
```

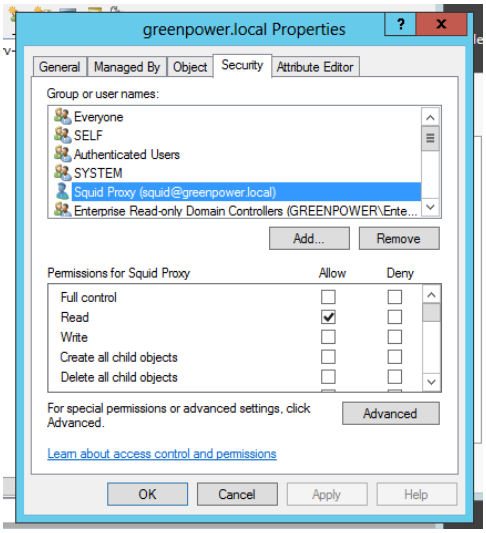
Gruppi d'accesso
L'autorizzazione ad utilizzare Internet è gestita tramite i gruppi in Active Directory.
Per default l'account squid non è abilitato ad interrogare l'attributo "MemberOf" che indica l'appartenenza di un utente ad un gruppo in AD.
per questo, bisogna configurare AD per concedere all'utente squid questo permesso.

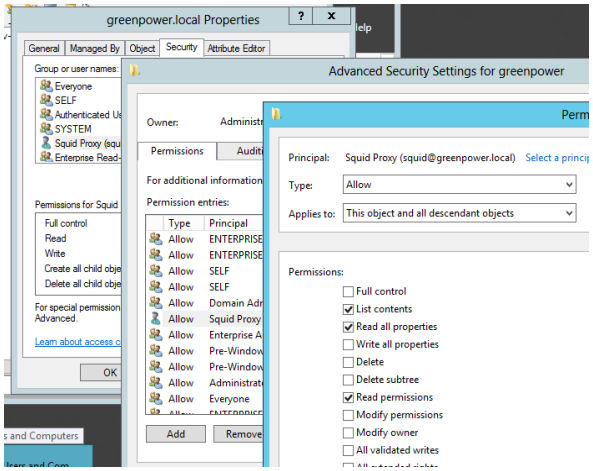
Active Directory User And Computers -> Nome del dominio -> tasto destro -> properties.
Security Tab -> aggiungere utente squid -> read permissions

In seguito, -> advanced -> squid proxy edit -> This Object and all descendant objects.



Attenzione, in 2008 e 2012 se non si vedesse il tab security, attivare Advanced features.





Definizione dei gruppi per i diritti d'accesso ad Internet in AD:
Definite i seguenti gruppi di sicurezza in AD ed aggiungetevi i rispettivi utenti. Per avere un certo ordine è meglio definire questi gruppi in un'apposita Unità Organizzativa, che chiameremo **User_Internet_Access** e che metteremo sotto la UO del dominio.

Gruppi da creare:

- **Internet_Users_Blocked**
  i membri di questo gruppo non avranno nessun accesso ad Internet.
- **Internet_Users_Restricted**
  i membri di questo gruppo avranno accesso solo ai siti permessi (White list)
- **Internet_Users_Standard**
  i membri di questo gruppo avranno accesso ad Internet salvo che ai siti bloccati (Black list)
- **Internet_Users_Exception**
  i membri di questo gruppo avranno accesso ad Internet ed ad alcune eccezioni nei siti bloccati (Exception black list)
- **Internet_Users_Full**
  i membri di questo gruppo avranno accesso totale ad Internet
- **Internet_Users_Anonymous**
  i membri di questo gruppo avranno accesso totale ad Internet e non saranno tracciati (logged)

Per meglio effettuare i test, suggerisco di aggiungere dapprima tutti gli utenti al gruppo **Internet_Users_Standard** e poi di alzare od abbassare il livello del loro accesso spostandoli da un gruppo all'altro.
L'ordine d'accesso è sempre dal meno restrittivo al più restrittivo. Se per esempio un utente fosse contemporaneamente membro dei gruppi Blocked, Standard e Anonymous, il gruppo Blocked avrebbe la priorità e l'utente non avrebbe mai l'accesso ad Internet (lettura dei permessi d'accesso in Squid dall'alto in basso).

Creazione dei files in Squid:
Bisogna creare dei files corrispondenti ai gruppi AD nei quali Squid leggerà l'appartenenza degli utenti.
Per fare più in fretta, invece dell'editore nano utilizzeremo il comando echo:

```
echo 'Internet_Users_Blocked' > /etc/squid3/blocked_access.txt
echo 'Internet_Users_Restricted' > /etc/squid3/restricted_access.txt
echo 'Internet_Users_Standard' > /etc/squid3/standard_access.txt
echo 'Internet_Users_Exception' > /etc/squid3/exception_access.txt
echo 'Internet_Users_Full' > /etc/squid3/full_access.txt
echo 'Internet_Users_Anonymous' > /etc/squid3/anonymous_access.txt
```

Dopo aver effettuato le modifiche, squid deve prenderle a carico:

```
invoke-rc.d squid3 reload
```

oppure:

```
/etc/init.d/squid3 reload
```

Configurazione di Squid:
Per poter negoziare l'autenticazione con Kerberos, Squid ha bisogno di un programma di supporto (helper) negotiate_wrapper.
Prima però è necessario installare i tools di compilazione:

```
apt-get install build-essential linux-headers-$(uname -r)
```

In seguito, scaricare e decomprimere il file negotiate_wrapper:

```
cd /usr/local/src/
wget
"http://downloads.sourceforge.net/project/squidkerbauth/negotiate_wrapper/negotia
te_wrapper-1.0.1/negotiate_wrapper-1.0.1.tar.gz"

tar -xvzf negotiate_wrapper-1.0.1.tar.gz
```

e poi, compilare ed installare:

```
cd negotiate_wrapper-1.0.1/
./configure
make
make install
```

Modifica di squid.conf:

Ora si tratta di modificare il file squid.conf ed i suoi files di configurazione associati.

Per prima cosa, salviamo il contenuto attuale del file squid.conf:

```
cp /etc/squid3/squid.conf /etc/squid3/squid.conf.default
```

poi lo editiamo:

```
nano /etc/squid3/squid.conf
```

ed aggiungiamo nella sezione auth_param:

```
### negotiate kerberos and ntlm authentication
auth_param negotiate program /usr/local/bin/negotiate_wrapper -d --ntlm
/usr/bin/ntlm_auth --diagnostics --helper-protocol=squid-2.5-ntlmssp --
domain=GREENPOWER --kerberos /usr/lib/squid3/squid_kerb_auth -d -s GSS_C_NO_NAME
auth_param negotiate children 10
auth_param negotiate keep_alive off

### pure ntlm authentication
auth_param ntlm program /usr/bin/ntlm_auth --diagnostics --helper-protocol=squid-
2.5-ntlmssp --domain=GREENPOWER
auth_param ntlm children 10
auth_param ntlm keep_alive off
```

```
### provide basic authentication via ldap for clients not authenticated via
kerberos/ntlm
auth_param basic program /usr/lib/squid3/basic_ldap_auth -R -b
"dc=greenpower,dc=local" -D squid@greenpower.local -W /etc/squid3/ldappass.txt -f
sAMAccountName=%s -h Nome_server_AD.greenpower.local
auth_param basic children 10
auth_param basic realm Internet Proxy
auth_param basic credentialsttl 1 minute

### ldap authorisation
external_acl_type memberof %LOGIN /usr/lib/squid3/ext_ldap_group_acl -R -K -S -b
"dc=greenpower,dc=local" -D squid@greenpower.local -W /etc/squid3/ldappass.txt -f
"(&(objectclass=person)(sAMAccountName=%v)(memberof=cn=%g,ou=Security
Groups,ou=greenpower,dc=greenpower,dc=local))" -h Nome_server_AD.greenpower.local
```

Attenzione, modificare a seconda dei propri nomi di dominio e di server Active Directory

Aggiungiamo nella sezione acl:

```
### acl for proxy auth and ldap authorizations
acl auth proxy_auth REQUIRED

#   aclname             acltype  typename activedirectorygroup
acl BlockedAccess       external memberof "/etc/squid3/blocked_access.txt"
acl RestrictedAccess    external memberof "/etc/squid3/restricted_access.txt"
acl StandardAccess      external memberof "/etc/squid3/standard_access.txt"
acl ExceptionAccess     external memberof "/etc/squid3/exception_access.txt"
acl FullAccess          external memberof "/etc/squid3/full_access.txt"
acl AnonymousAccess     external memberof "/etc/squid3/anonymous_access.txt"
acl allowedsites        dstdomain "/etc/squid3/allowedsites.txt"
acl blockedsites        dstdomain "/etc/squid3/blockedsites.txt"
acl exceptedsites       dstdomain "/etc/squid3/exceptedsites.txt"
acl prioritysites       dstdomain "/etc/squid3/prioritysites.txt"
```

Aggiungiamo alla sezione http_access:

```
### http_access rules
# allow unrestricted access to prioritysites
http_access allow prioritysites

# enforce authentication, order of rules is important for authorization levels
http_access deny !auth

# prevent access to basic auth prompt for BlockedAccess users
http_access deny BlockedAccess all
http_access allow allowedsites
http_access deny RestrictedAccess all
http_access allow AnonymousAccess auth
http_access allow FullAccess auth
http_access allow ExceptionAccess exceptedsites auth
http_access deny blockedsites
http_access allow StandardAccess auth
# DO NOT REMOVE THE FOLLOWING LINE
http_access deny all
```

ed infine definiamo che le seguenti liste di siti non dovranno apparire nei logs (opzionale)

```
### logging
# don't log allowedsites, prioritysites, AnonymousAccess
access_log /var/log/squid3/access.log
squid !allowedsites !prioritysites !AnonymousAccess
```

Se il servizio Squid non dovesse partire, probabilmente ci saranno degli errori di sintassi nel file squid.conf.
Per controllarlo, utilizzare il comando `squid3 -k parse` e controllare gli eventuali errori annunciati.

Ora bisogna creare i files che conterranno le liste dei siti bloccati, permessi ecc:

```
touch /etc/squid3/allowedsites.txt
touch /etc/squid3/blockedsites.txt
touch /etc/squid3/exceptedsites.txt
touch /etc/squid3/prioritysites.txt
```

Questi files andranno poi completati inserendo la lista dei siti corrispondenti, per esempio, per i siti bloccati potremmo editare il file:

```
nano /etc/squid3/blockedsites.txt
```

ed aggiungere:

```
### How to add domains to this file
#
#   1.  Use only the domain name EXCLUDING the protocol prefix, i.e.
#       don't put "http://" at the start.
#
#   2.  Do not append a directory to the domain name, i.e. don't put
#       /index.php/path/blah.html at the end of the name.
#
#   3.  Prefix each entry with a single dot ".", this ensures a match of
#       example.com and www.example.com.
#
#   4.  If you need to match different top level domains like .com,
#       .net, .com.au for sites that have multiple top level domains to
#       the same website then add a seperate entry for each e.g.
#           .example.com
#           .example.com.au
#
###
.youtube.com
.facebook.com
.twitter.com
```

La medesima cosa la si potrà fare con i file per i siti permessi, prioritari e di eccezione.

Attenzione:
il file priroritysites.txt conterrà una lista di siti per l'aggiornamento degli antivirus, del sistema operativo ecc. Questi siti saranno completamente aperti e senza restrizioni per tutti i clients. Bisognerà quindi fare attenzione a quello che viene inserito.

Alla fine riavviare squid:

```
service squid3 restart
```

Controllate si vi sono errori e provate l'accesso da diversi clients.
Dovessero esserci problemi, controllate i log files `/var/log/squid3/access.log` e `/var/log/squid3/cache.log`

Eventuali altre configurazioni per migliorare il confort di utilizzazione anche da parte degli utenti:

- Auto configurazione del proxy tramite file `wpad.dat`
- Inserimento di un logo nella pagina di annuncio d'errore
- Possibilità di delegare ad alcuni collaboratori l'editazione delle liste "blockedsites" e whitelistsites" tramite browser.
- Installazione di Cyphin Reporter

Sito di riferimento:
http://wiki.bitbinary.com/index.php/Active_Directory_Integrated_Squid_Proxy