# Squid и авторизация пользователей в AD

## Вступление

Очень часто в средних и крупных организациях используют AD (здесь и далее AD - Active Directory). Но, как правило, на шлюзах ставят unix-like системы FreeBSD/Linux и т.п. Для выхода в интернет локальной сети используют два варианта: NAT (Network Address Translation) и прокси сервер. Рассмотрим второй случай, когда для выхода используется прокси сервер (squid).

Для ограничения доступа к прокси серверу необходимо настроить аутентификацию пользователей. Squid поддерживает очень много схем аутентификации, но при наличии AD самым разумным и оптимальным было бы сделать так, чтобы squid брал информацию прямо из AD. При таком методе мы получаем единое хранилище учетных записей. При большом количестве пользователей 50 и более это очень удобно и эффективно. Так как нам не надо заводить для каждого пользователя отдельную учетную запись на шлюзе.

Для реализации данной задачи нам понадобятся следующие пакеты:

- samba - необходима для аутентификации пользователей в AD.
- squid - кэширующий прокси сервер.

**Исходные данные**
Контроллер домена - windows 2000 server SP4, Native mode.
freebsd 5.4 - шлюз, на котором мы и будем настраивать прокси сервер.
192.168.127.0/24 - наша локальная сеть.
192.168.127.1 - ip контроллера домена.
192.168.127.230 - внутренний ip шлюза.

Перед началом настройки данной связки рекомендую обновить дерево портов. Как это сделать, читаем здесь

## Samba

Итак, начнем по порядку. Собираем самбу.

```
# cd /usr/ports/net/samba3/
# make config

Options for samba 3.0.21a,1

[X] LDAP          With LDAP support
[X] ADS           With Active Directory support
[ ] CUPS          With CUPS printing support
[X] WINBIND       With WinBIND support
[ ] ACL_SUPPORT   With ACL support
[ ] AIO_SUPPORT   With experimental AIO support
```

```
[ ] SYSLOG        With Syslog support
[ ] QUOTAS        With Quota support
[ ] UTMP          With UTMP support
[ ] MSDFS         With MSDFS support
[ ] SAM_XML       With XML support smbpasswd backend
[ ] SAM_MYSQL     With MYSQL smbpasswd backend
[ ] SAM_PGSQL     With PostgreSQL support smbpasswd backend
[ ] SAM_OLD_LDAP  With Samba2.x LDAP smbpasswd backend
[ ] PAM SMBPASS   With SMB PAM module
[ ] POPT          With installed POPT library

# make install clean
# rehash
```

При конфигурации обращаем внимание на следующие строчки <code bash> … checking for LDAP support… yes … checking whether LDAP support is used… yes checking for Active Directory and krb5 support… yes … checking whether Active Directory and krb5 support is used… yes … </cli> Создаем конфигурационный файл и настраиваем самбу

```
# cd /usr/local/etc
# cp smb.conf.default smb.conf
```

```
#
#   /usr/local/etc/smb.conf
#

#======================= Global Settings =======================
[global]

# netbios имя домена
workgroup = TURBOGAZ

# Строка комментария
server string = Turbogaz Proxy Server

# Режим безопасности, в нашем случае ads
security = ads

# Разрешаем доступ только с нашей сети
hosts allow = 192.168.127.

# расположение лог файла и его размер
log file = /var/log/samba/samba.log
max log size = 500

# Здесь необходимо указать dns имя или ip контроллера домена,
# если указываете dns имя необходимо убедиться, что разрешение
# имен работает правильно
password server = server.turbogaz.net

# dns имя Active Directory
```

```
realm = turbogaz.net

# Тип хранилища.
passdb backend = tdbsam

# Сетевые настройки.
socket options = TCP_NODELAY

# Указываем, что самба не является  PDC
local master = no
domain master = no
preferred master = no
domain logons = no
os level = 0

# Настройка кириллицы
display charset = koi8-r
unix charset = koi8-r
dos charset = cp866

# Использовать шифрованные пароли
encrypt passwords = yes

# Настройки winbind
winbind use default domain = no
winbind uid = 10000-20000
winbind gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
```

Теперь необходимо изменить nsswitch.conf, чтобы winbind смог получать информацию из AD

```
# cat /etc/nsswitch.conf | grep winbind
group: files winbind
passwd: files winbind
```

Проверяем работу dns и производим синхронизацию времени

```
# nslookup server.turbogaz.net
Server:         192.168.127.1
Address:        192.168.127.1#53

Name:   server.turbogaz.net
Address: 192.168.127.1

# net time set
Tue Jan 31 22:04:51 EET 2006
```

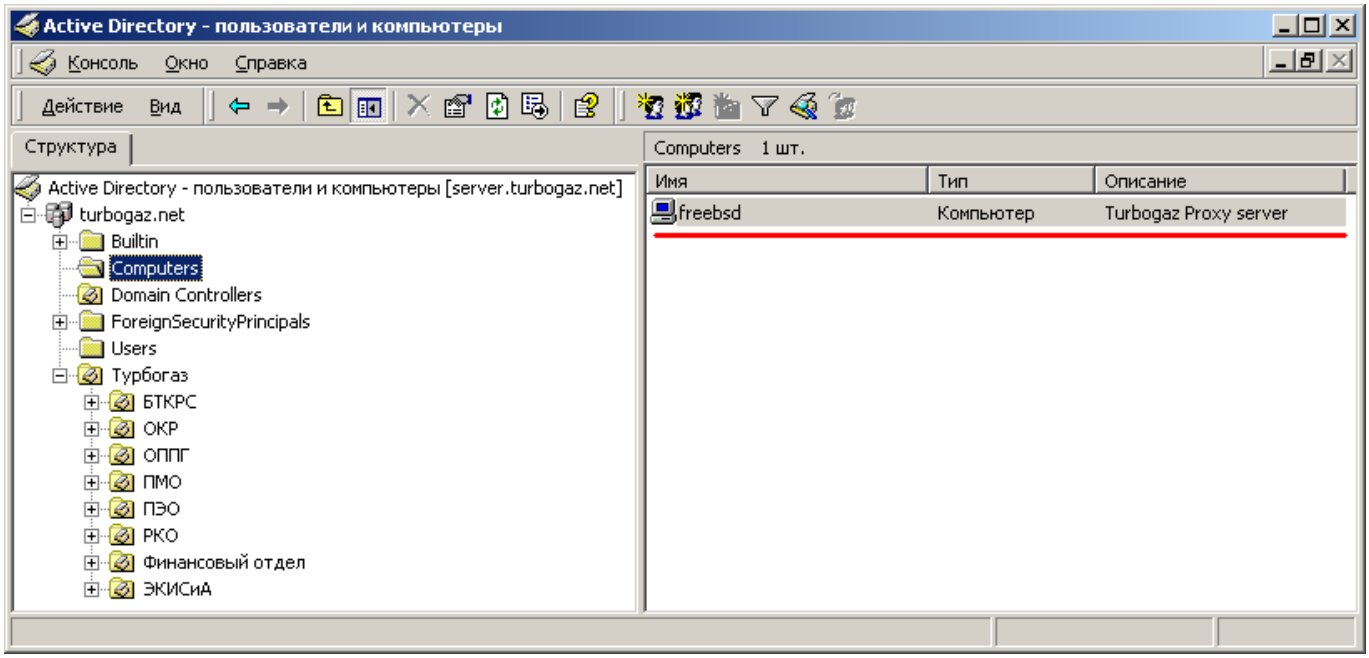
Теперь у нас все готово для ввода машины в домен

```
# net ads join -U DomoradovA%123456
```

```
Using short domain name -- TURBOGAZ
Joined 'FREEBSD' to realm 'TURBOGAZ.NET'
```

Пользователь DomoradovA - должен обладать правом добавлять машины в домен. Естественно вы должны использовать своего пользователя. Во избежание проблем настоятельно рекомендую не использовать русские символы в логине и пароле.

Как видно из сообщения машина добавлена в домен. Для того, чтобы убедиться в этом необходимо открыть оснастку - «Active Directory - пользователи и компьютеры»




Настраиваем запуск winbind вместе с системой, а также включаем режим отладки, облегчающий найти и устранить неисправность.

```
# echo 'winbindd_enable="YES"' >> /etc/rc.conf
# echo 'winbindd_flags="-d 3"' >> /etc/rc.conf
```

Примечание !!! Для работы данной связки запускать smbd и nmbd нет необходимости. Поэтому для экономии ресурсов я специально не прописывал их. Примечание !!! На время тестирования и поиска неисправностей лучше указывать большой уровень информативности 7-9. При этом уровне, в логах будет очень много полезной информации, которая в 95% случаев поможет найти ошибку. После того, как вы полнсотью настроили данную связку, отладку можно вообще выключить или задать самый маленький уровень информативности - 1.

Запускаем winbind.

```
# /usr/local/etc/rc.d/samba.sh start
Starting winbindd.
```

Теперь для проверки работоспособности winbind проведем ряд тестов. Для этого воспользуемся программой wbinfo

```
# wbinfo -p
Ping to winbindd succeeded on fd 4
```

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

```
# wbinfo -u
TURBOGAZ\domoradova
TURBOGAZ\администратор
TURBOGAZ\гость
TURBOGAZ\tsinternetuser
TURBOGAZ\krbtgt
TURBOGAZ\freebsd$
TURBOGAZ\server$
```

```
# wbinfo -g
TURBOGAZ\компьютеры домена
TURBOGAZ\контроллеры домена
TURBOGAZ\администраторы схемы
TURBOGAZ\администраторы предприятия
TURBOGAZ\издатели сертификатов
TURBOGAZ\администраторы домена
TURBOGAZ\пользователи домена
TURBOGAZ\гости домена
TURBOGAZ\владельцы-создатели групповой политики
TURBOGAZ\серверы ras и ias
TURBOGAZ\dnsadmins
TURBOGAZ\dnsupdateproxy
```

Если у вас такие же результаты, то значит все нормально и winbind работает правильно. Теперь просмотрим информацию о домене и AD.

```
# wbinfo -D TURBOGAZ
Name               : TURBOGAZ
Alt_Name           : turbogaz.net
SID                : S-1-5-21-220523388-842925246-839522115
Active Directory   : Yes
Native             : Yes
Primary            : Yes
Sequence           : 3143
```

```
# net ads info
LDAP server: 192.168.127.1
LDAP server name: server
Realm: TURBOGAZ.NET
Bind Path: dc=TURBOGAZ,dc=NET
LDAP port: 389
Server time: Tue, 31 Jan 2006 22:34:27 EET
KDC server: 192.168.127.1
Server time offset: -7
```

Проверим аутентификацию

```
# wbinfo --authenticate=TURBOGAZ\\DomoradovA%123456
plaintext password authentication succeeded
challenge/response password authentication succeeded
```

Проверим утилитой id доменного пользователя

```
# id TURBOGAZ\\DomoradovA
uid=10000(TURBOGAZ\domoradova) gid=10005(TURBOGAZ\администраторы домена)
groups=10005(TURBOGAZ\администраторы домена), 10006(TURBOGAZ\пользователи
домена)
```

Если у вас такие же результаты, то поздравляю, самбу мы настроили. Теперь осталось только указать пользователя, от имени которого будет проходить аутентификация.

```
# wbinfo --set-auth-user=TURBOGAZ\\DomoradovA%123456
# wbinfo --get-auth-user
TURBOGAZ\DomoradovA%123456
```

# Squid

Собираем и настраиваем squid

```
# cd /usr/ports/www/squid/
# make config

Options for squid 2.5.12_3

[ ] SQUID_LDAP_AUTH        Install LDAP authentication helpers
[X] SQUID_DELAY_POOLS      Enable delay pools
[X] SQUID_SNMP             Enable SNMP support
[ ] SQUID_CARP             Enable CARP support
[X] SQUID_SSL              Enable SSL support for reverse proxies
[X] SQUID_PINGER           Install the icmp helper
[ ] SQUID_DNS_HELPER       Use the old 'dnsserver' helper
[X] SQUID_HTCP             Enable HTCP support
[ ] SQUID_VIA_DB           Enable forward/via database
[X] SQUID_CACHE_DIGESTS    Enable cache digests
[X] SQUID_WCCP             Enable Web Cache Coordination Protocol
[ ] SQUID_UNDERSCORES      Allow underscores in hostnames
[X] SQUID_CHECK_HOSTNAME   Do hostname chechking
[ ] SQUID_STRICT_HTTP      Be strictly HTTP compliant
[X] SQUID_IDENT            Enable ident (RFG 931) lookups
[ ] SQUID_USERAGENT_LOG    Enable User-Agent-header logging
[X] SQUID_ARP_ACL          Enable ACLs based on ethernet address
[ ] SQUID_PF               Enable transparent proxying with PF
[ ] SQUID_IPFILTER         Enable transp. proxying with IPFilter
[ ] SQUID_FOLLOW_XFF       Follow X-Forfarded-For headers
[ ] SQUID_ICAP             Enable ICAP client functionality
```

```
[ ] SQUID_AUFS             Enable the aufs storage scheme
[ ] SQUID_COSS             Enable the COSS storage scheme
[ ] SQUID_LARGEFILE        Support log and cache files >2GB
[ ] SQUID_STACKTRACES      Create backtraces on fatal errors
[X] SQUID_RCNG             Install an rcNG startup script

# make install clean
```

Производим минимальную настройку squid. Все изменения необходимо вводить после соответствующих тегов.

```
#
#   /usr/local/etc/squid/squid.conf
#

#  TAG: http_port
# Указываем squid на каком порту и интерфейсе он будет работать. Именно эти
# параметры необходимо будет указывать в настройках интернет проводника.
http_port 192.168.127.230:3128

#  TAG: maximum_object_size_in_memory   (bytes)
# Объекты больше этого размера не будут сохраняться в памяти.
# По умолчанию 8КБ что очень мало на текущий момент, т.к. средний объем
# web странички ~75-100 КБ
maximum_object_size_in_memory 102400

#  TAG: cache_dir
# Объем кеша и его месторасположение. Объем задается в мегабайтах. (4096 ~ 4Гб)
cache_dir ufs /usr/local/squid/cache 4096 16 256

#  TAG: dns_nameservers
# Здесь необходимо указать днс сервер(а). В принципе если ничего не указывать,
# то squid автоматически добавит сервер(а), которые указаны в /etc/resolv.conf
# Я указал адрес самого сервера, т.к. у меня на нем работает кеширующий днс.
# Если у вас нет своего днс сервера, то необходимо указывать днс провайдера.
dns_nameservers 192.168.127.230

# TAG: auth_param
# Здесь мы указываем squid как следуею производить аутентификацию и настраиваем
# соответствущие схемы аутентифиуации. Внимание: порядок описания схем имеет
# значение, поэтому первой должна идти ntlm аутентификация.
# С помощью таких настроек мы разрешили доступ к прокси серверу только для
# пользователей группы InternetUsers. Если нам необходимо закрыть доступ
# определенному человеку, мы просто удалим его из группы InternetUsers.
auth_param ntlm program /usr/local/bin/ntlm_auth --helper-protocol=
squid-2.5-ntlmssp --require-membership-of=TURBOGAZ\\InternetUsers
auth_param ntlm children 5
auth_param ntlm max_challenge_reuses 0
auth_param ntlm max_challenge_lifetime 2 minutes
auth_param ntlm use_ntlm_negotiate off
```

```
auth_param basic program /usr/local/bin/ntlm_auth --helper-protocol=
squid-2.5-basic --require-membership-of=TURBOGAZ\\InternetUsers
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
auth_param basic casesensitive off

# TAG: acl
# ACL - Access Control List. Списки доступа к нашему прокси серверу.
# Здесь мы указываем кто имеет право, а кто нет, использовать наш прокси.
# ACL очень гибкое и мощное средство разграничения прав, но лично я для этих
# целей использую редиректор squidGuard.
# Разрешаем использовать наш прокси только прошедшим авторизацию.
acl TURBOGAZ proxy_auth REQUIRED
http_access allow TURBOGAZ
http_access deny all

#  TAG: cache_effective_user
# Пользователь и группа, от которых работает squid
cache_effective_user squid

#  TAG: cache_effective_group
cache_effective_group squid

#  TAG: visible_hostname
# Данное имя будет указываться в различных сообщениях (об ошибках и т.п.)
# По умолчанию будет подставляться значение, возвращаемое функцией gethostname()
visible_hostname turbogaz.proxy.server
```

Это лишь минимальная настройка, на самом деле, squid имеет очень много параметров конфигурации. К счастью squid.conf имеет очень хорошие комментарии к каждому из параметров.

О том, как настроить squidGuard читаем здесь.

Если вы впервый раз запускаете squid, то перед запуском необходимо создать иерархию папок для кеша. Для этого запускаем squid со следующими ключами:

```
# squid -D -d 3 -z
2006/03/19 17:50:02| Creating Swap Directories
```

Ну а теперь настало время проверить нашу связку, но перед этим необходимо выставить права на папку winbind_privileged, иначе squid не сможет проводить аутентификацию.

```
# chown -R root:squid /var/db/samba/winbindd_privileged/
# chmod -R 750 /var/db/samba/winbindd_privileged/
```

Настраиваем запуск squid вместе с системой

```
# echo 'squid_enable="YES"' >> /etc/rc.conf
```

Запускаем squid и смотрим логи

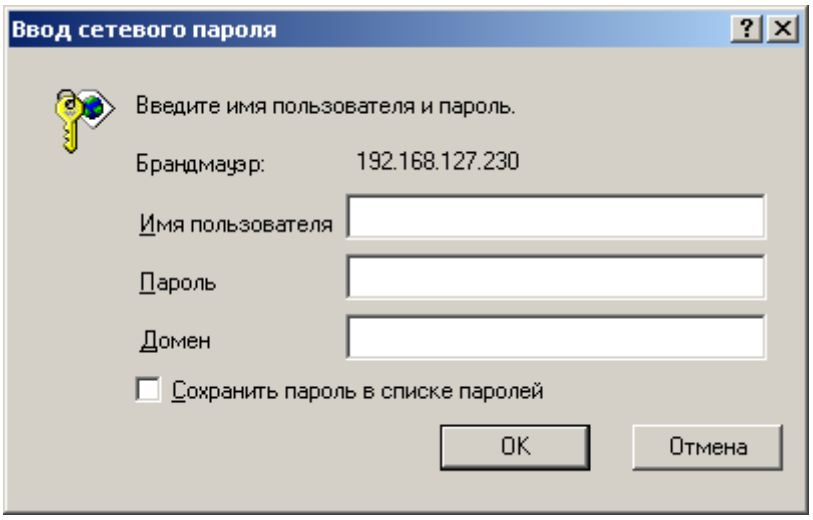
```
# /usr/local/etc/rc.d/squid.sh start
Starting squid.

# cat /usr/local/squid/logs/cache.log
2006/03/19 17:59:14| Starting Squid Cache version 2.5.STABLE12
for i386-portbld-freebsd5.4...
2006/03/19 17:59:14| Process ID 72232
2006/03/19 17:59:14| With 7296 file descriptors available
2006/03/19 17:59:14| DNS Socket created at 0.0.0.0, port 50201, FD 5
2006/03/19 17:59:14| Adding nameserver 192.168.127.230 from squid.conf
2006/03/19 17:59:14| helperStatefulOpenServers: Starting 5 'ntlm_auth'
processes
2006/03/19 17:59:14| helperOpenServers: Starting 5 'ntlm_auth' processes
2006/03/19 17:59:14| User-Agent logging is disabled.
2006/03/19 17:59:14| Unlinkd pipe opened on FD 10
2006/03/19 17:59:14| Swap maxSize 4194304 KB, estimated 322638 objects
2006/03/19 17:59:14| Target number of buckets: 393
2006/03/19 17:59:14| Using 16384 Store buckets
2006/03/19 17:59:14| Max Mem  size: 8192 KB
2006/03/19 17:59:14| Max Swap size: 102400 KB
2006/03/19 17:59:14| Local cache digest enabled; rebuild/rewrite every 3600
sec
2006/03/19 17:59:14| Rebuilding storage in /usr/local/squid/cache (DIRTY)
2006/03/19 17:59:14| Using Least Load store dir selection
2006/03/19 17:59:14| Set Current Directory to /usr/local/squid/cache
2006/03/19 17:59:14| Loaded Icons.
2006/03/19 17:59:14| Accepting HTTP connections at 192.168.127.230, port
3128, FD 11.
2006/03/19 17:59:14| Accepting ICP messages at 0.0.0.0, port 3130, FD 12.
2006/03/19 17:59:14| Accepting HTCP messages on port 4827, FD 13.
2006/03/19 17:59:14| Accepting SNMP messages on port 3401, FD 14.
2006/03/19 17:59:14| Ready to serve requests.
2006/03/19 17:59:20| Done scanning /usr/local/squid/cache (0 entries)
2006/03/19 17:59:20| Finished rebuilding storage from disk.
2006/03/19 17:59:20|         0 Entries scanned
2006/03/19 17:59:20|         0 Invalid entries.
2006/03/19 17:59:20|         0 With invalid flags.
2006/03/19 17:59:20|         0 Objects loaded.
2006/03/19 17:59:20|         0 Objects expired.
2006/03/19 17:59:20|         0 Objects cancelled.
2006/03/19 17:59:20|         0 Duplicate URLs purged.
2006/03/19 17:59:20|         0 Swapfile clashes avoided.
2006/03/19 17:59:20|   Took 6.5 seconds (   0.0 objects/sec).
2006/03/19 17:59:20| Beginning Validation Procedure
2006/03/19 17:59:21|   Completed Validation Procedure
2006/03/19 17:59:21|   Validated 0 Entries
2006/03/19 17:59:21|   store_swap_size = 0k
2006/03/19 17:59:21| storeLateRelease: released 0 objects
```

# Тестирование

В настройках любимого интернет проводника указываем адрес нашего прокси и проверяем его работу. Если все правильно настроено, то в логах должно быть следующее

```
# cat /usr/local/squid/logs/access.log
1138745487.991    354 192.168.127.1 TCP_IMS_HIT/304 283
GET http://192.168.127.230/ TURBOGAZ\domoradova NONE/- text/html
```

Теперь удалим пользователя из группы InternetUsers и повторим попытку. При этом на экране должно появиться следующее окно авторизации. Независимо от того, какие данные будем вводить мы должны увидеть подобную страничку




При этом в логах должно быть следующее

```
# cat /usr/local/squid/logs/access.log | grep DENIED
1138746473.277      3 192.168.127.10 TCP_DENIED/407 1805
GET http://192.168.127.230/test.php - NONE/- text/html
1138746473.300     21 192.168.127.10 TCP_DENIED/407 1801
GET http://192.168.127.230/test.php - NONE/- text/html
```