RADIUS-

1.6.3750 WNAM RADIUS.

(NAS) TACACS+, -, , . TACACS+ / (MAB, EAP, ..).

, TACACS+. RADIUS. , CheckPoint. RADIUS- ; Plaintext (PAP) , - . CheckPoint. :

- CheckPoint RADIUS-,
- RADIUS- WNAM
- WNAM (RADIUS), , -
- Identity/Calling-Station-Id -, ( )
- , WNAM , "LAN Switch"

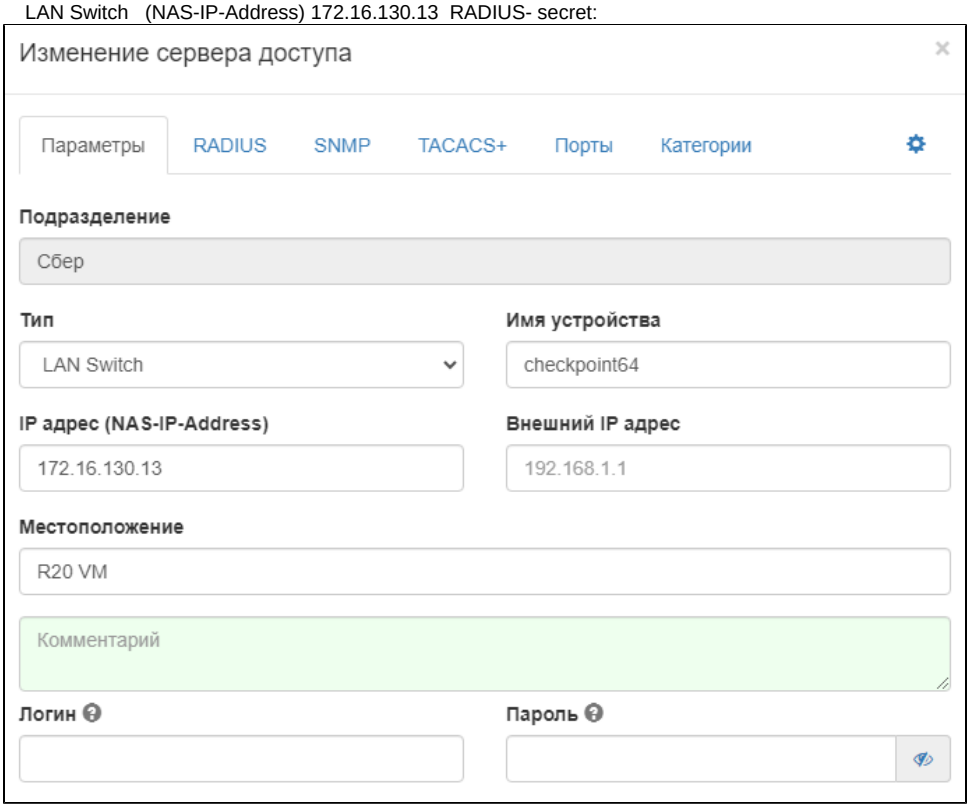
> Aruba , , Service-Type=6 Aruba-Priv-Admin-User=15 Aruba-Admin-Role=admin.
>
> RADIUS- .

, 172.16.130.0/24 172.16.130.13, :

- **pupkin**, WNAM ,
- **wifitest**, ActiveDirectory "lab.wnam.ru" ,

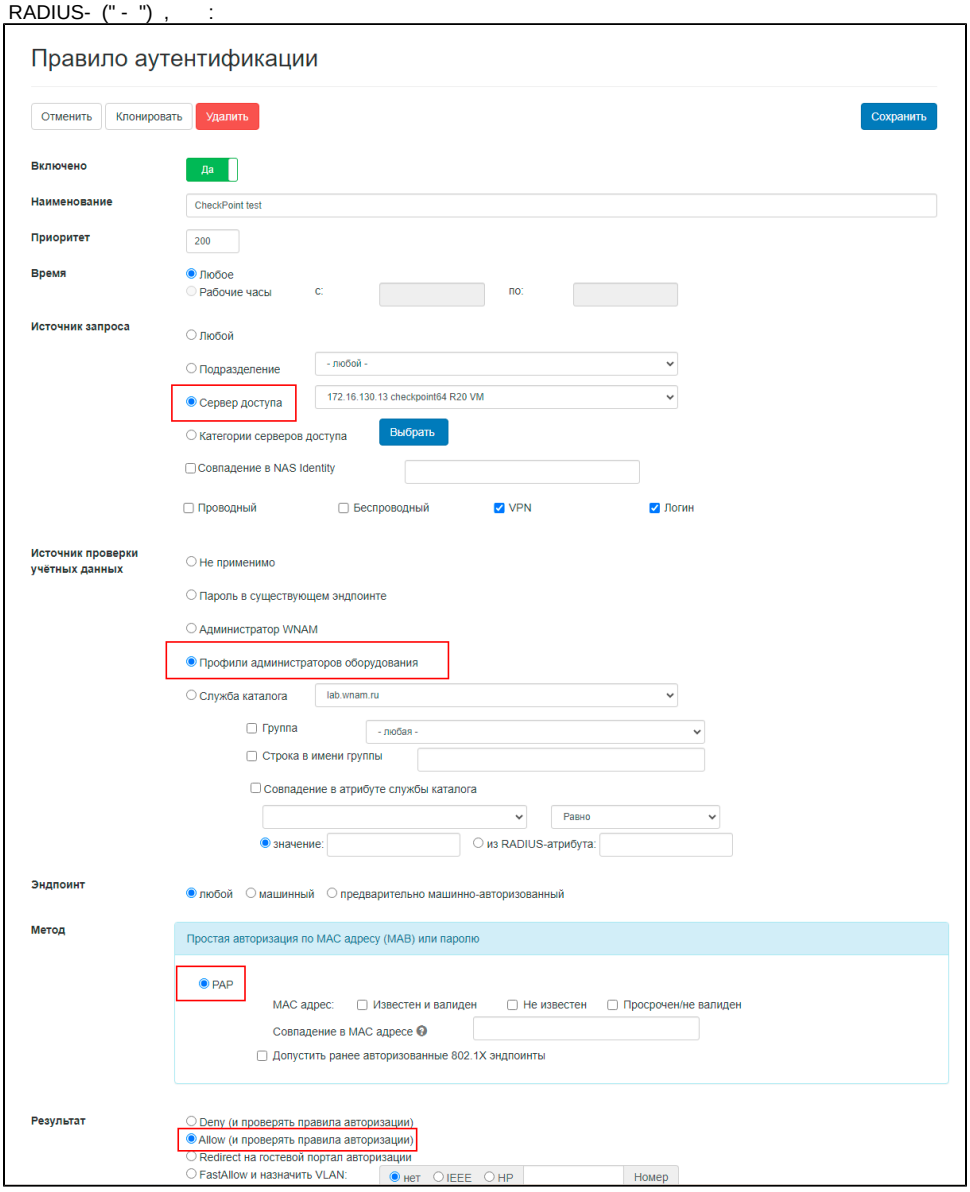
WNAM :

1. LAN Switch (NAS-IP-Address) 172.16.130.13 RADIUS- secret:

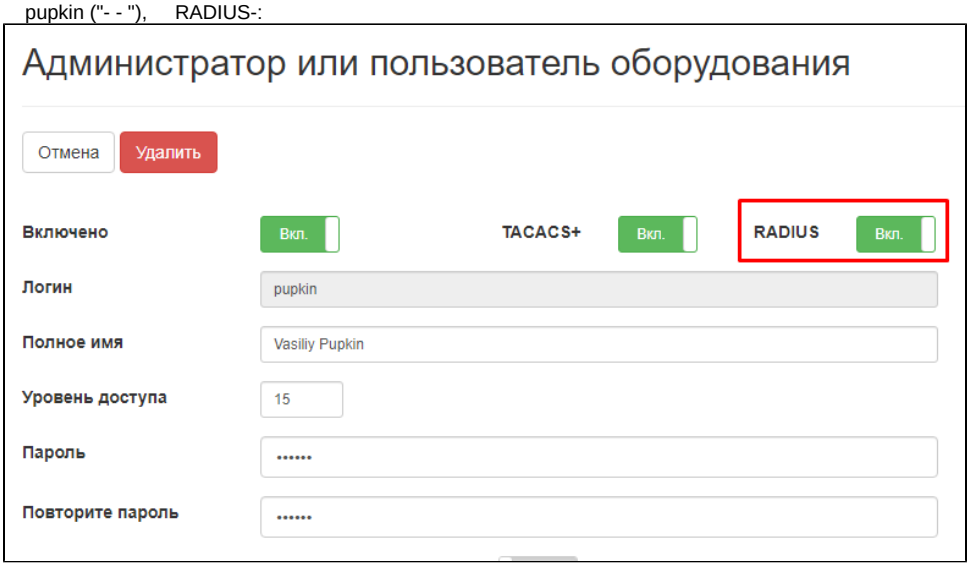


2. - (,)
3. ADCTool lab.wnam.ru

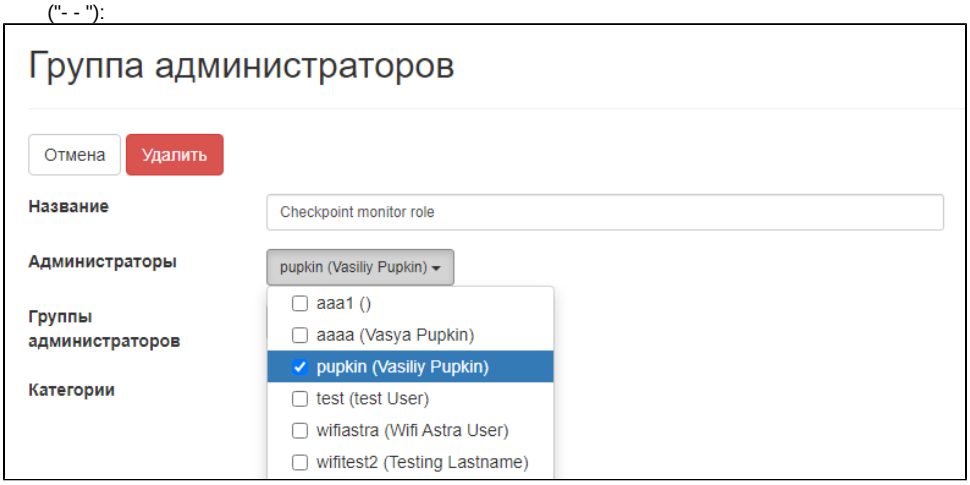
4. RADIUS- (" - ") , :



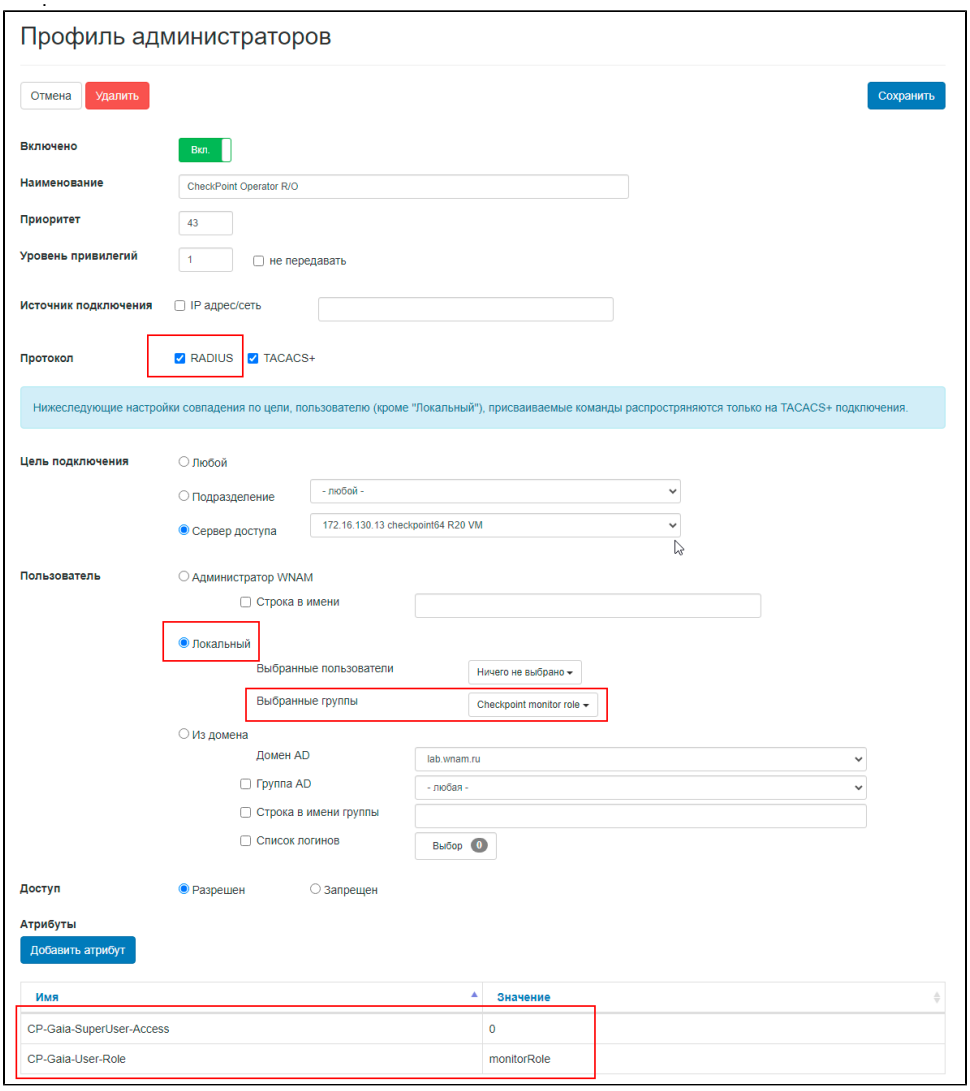
5. pupkin ("- - "), RADIUS-:



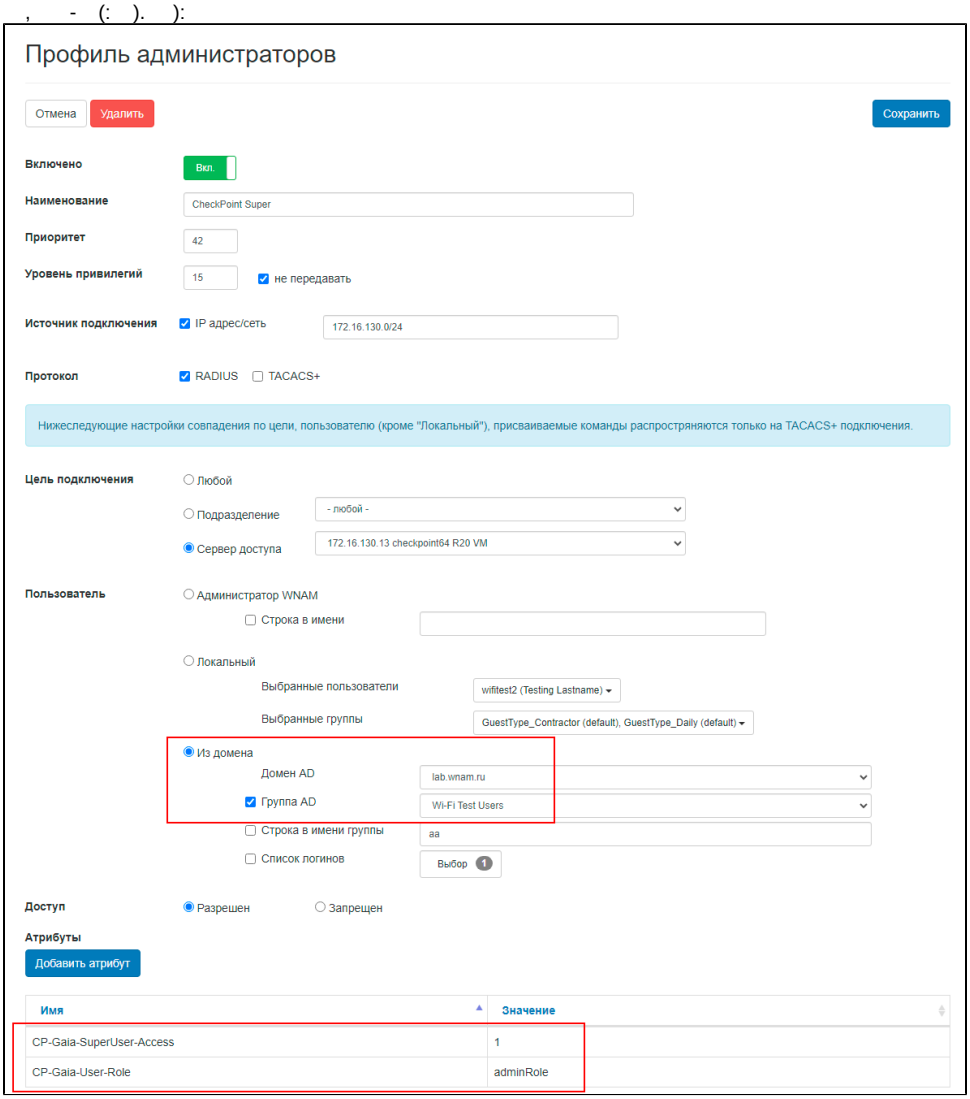
6. ("- - "):


Группа администраторов
Отмена
Удалить
Название
Checkpoint monitor role
Администраторы
pupkin (Vasiliy Pupkin)
Группы администраторов
Категории
aaa1 ()
aaaa (Vasya Pupkin)
pupkin (Vasiliy Pupkin)
test (test User)
wifiastra (Wifi Astra User)
wifitest2 (Testing Lastname)

7. , , ("- - ").
:


Профиль администраторов
Отмена
Удалить
Сохранить
Включено
Вкл.
Наименование
CheckPoint Operator R/O
Приоритет
43
Уровень привилегий
1
не передавать
Источник подключения
IP адрес/сеть
Протокол
RADIUS
TACACS+
Нижеследующие настройки совпадения по цели, пользователю (кроме "Локальный"), присваиваемые команды распространяются только на TACACS+ подключения.
Цель подключения
Любой
Подразделение
- любой -
Сервер доступа
172.16.130.13 checkpoint64 R20 VM
Пользователь
Администратор WNAM
Строка в имени
Локальный
Выбранные пользователи
Ничего не выбрано
Выбранные группы
Checkpoint monitor role
Из домена
Домен AD
lab.wnam.ru
Группа AD
- любая -
Строка в имени группы
Список логинов
Выбор
0
Доступ
Разрешен
Запрещен
Атрибуты
Добавить атрибут
Имя
Значение
CP-Gaia-SuperUser-Access
0
CP-Gaia-User-Role
monitorRole

8. , - (:).):

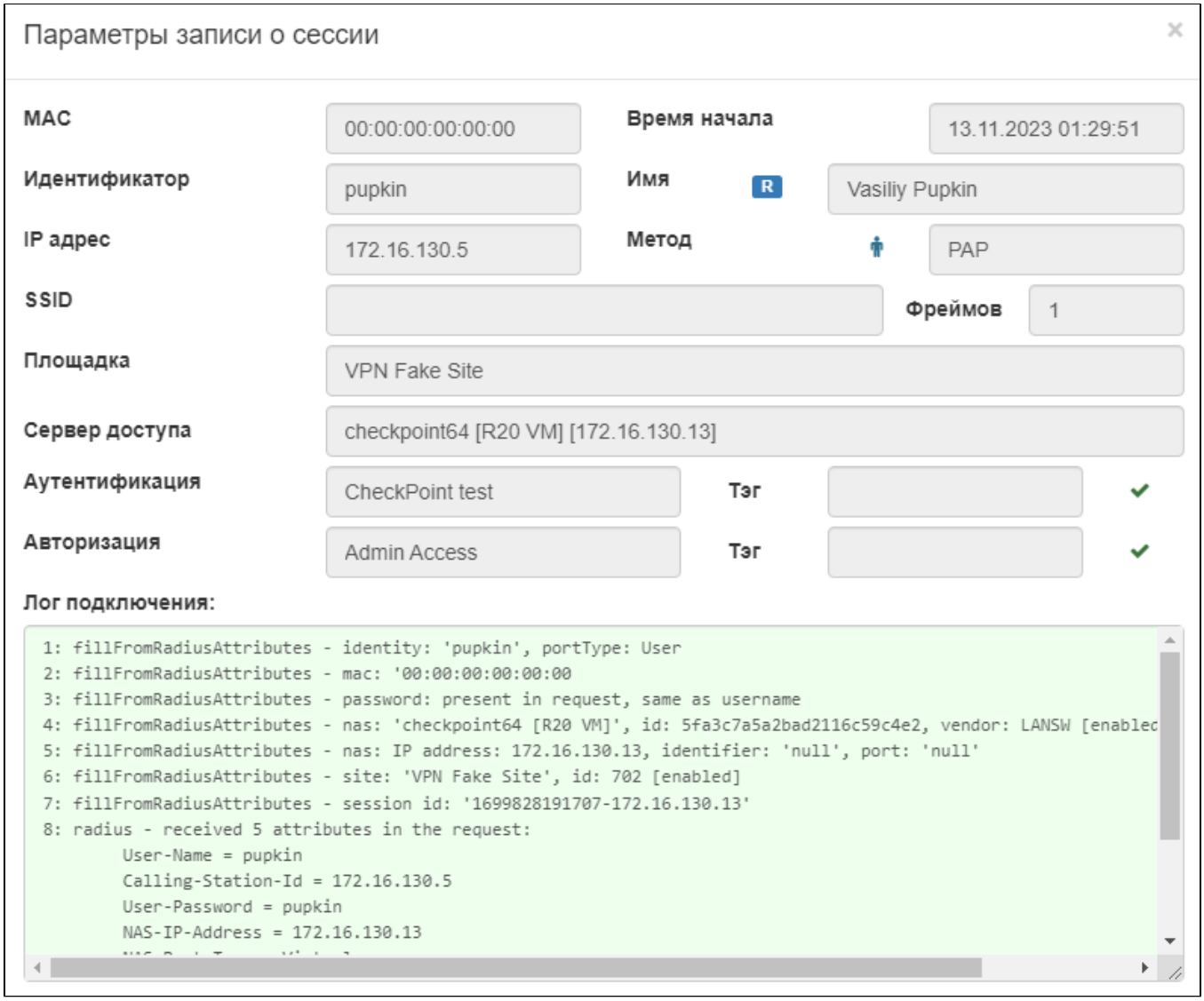


.

1. :

```
root@debian64:~# echo User-Name=pupkin,User-Password=pupkin,NAS-IP-Address=172.
16.130.13,NAS-Port-Type=Virtual,Calling-Station-Id=172.16.130.5 | radclient -x -
n 1 -t 10 172.16.130.5 auth secret
Sent Access-Request Id 215 from 0.0.0.0:47714 to 172.16.130.5:1812 length 72
 User-Name = "pupkin"
 User-Password = "pupkin"
 NAS-IP-Address = 172.16.130.13
 NAS-Port-Type = Virtual
 Calling-Station-Id = "172.16.130.5"
 Cleartext-Password = "pupkin"
Received Access-Accept Id 215 from 172.16.130.5:1812 to 172.16.130.13:47714
length 51
 CP-Gaia-User-Role = "monitorRole"
 CP-Gaia-SuperUser-Access = 0
```

"- " :



, :

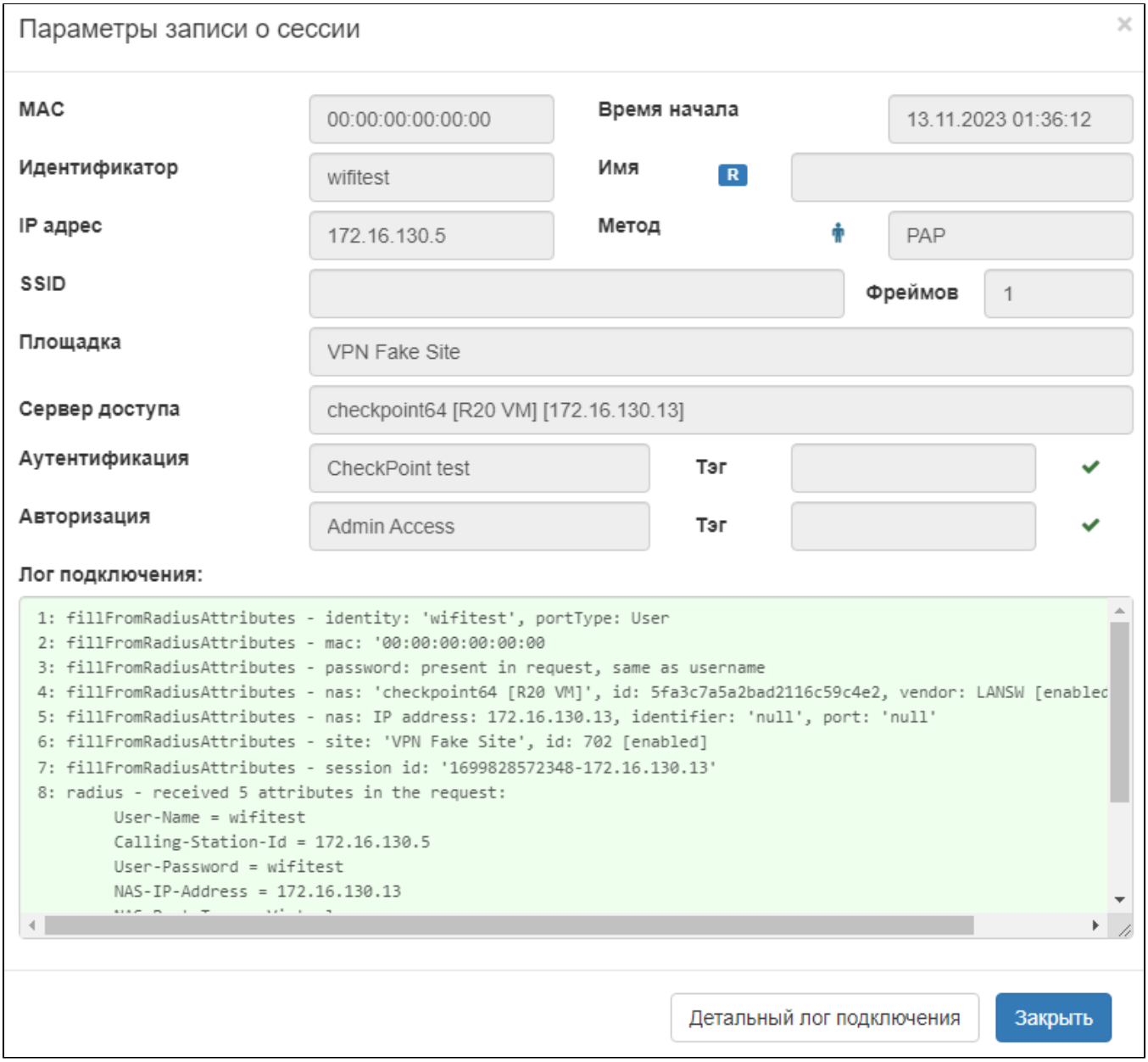
```
00.015 filterForA1Method - single candidate left: 'CheckPoint test'
00.016 filterForPapMacMethod - MAC state: exist: false, expired: false
00.022 local-admins-profiles - radius auth: username: 'pupkin', password: ***,
from: 172.16.130.5
00.022 local-admins-profiles - getAuthentication found local user, enabled:
true, r+ allowed: true
00.022 local-admins-profiles - !!! WNAM admin or local user is found; don't
request AD for domain profile: CheckPoint Super
00.022 local-admins-profiles - getAuthentication pcandidates left: 1
00.022 local-admins-profiles - getAuthentication profile 'CheckPoint Operator R
/O'
00.022 filterForPapMacMethod - CheckLocalAdminProfiles user 'pupkin' matched,
state: OK_SKIP, admin profile: 'CheckPoint Operator R/O'
```

2. :

```
root@debian64:~# echo User-Name=wifitest,User-Password=wifitest,NAS-IP-
Address=172.16.130.13,NAS-Port-Type=Virtual,Calling-Station-Id=172.16.130.5 |
radclient -x -n 1 -t 10 172.16.130.5 auth secret
Sent Access-Request Id 240 from 0.0.0.0:41290 to 172.16.130.5:1812 length 74
```

```
 User-Name = "wifitest"
 User-Password = "wifitest"
 NAS-IP-Address = 172.16.130.13
 NAS-Port-Type = Virtual
 Calling-Station-Id = "172.16.130.5"
 Cleartext-Password = "wifitest"
Received Access-Accept Id 240 from 172.16.130.5:1812 to 172.16.130.13:41290
length 49
 CP-Gaia-User-Role = "adminRole"
 CP-Gaia-SuperUser-Access = 1
```

"-" :



, :

```
00.470 local-admins-profiles - radius auth: username: 'wifitest', password: ***,
from: 172.16.130.5
00.470 local-admins-profiles - getAuthentication prio=42,
method=ACTIVE_DIRECTORY, pcandidate=CheckPoint Super
00.470 local-admins-profiles - getAuthentication checkInDomain lab.wnam.ru,
```

```
group_list=2 groups for that user
00.470 local-admins-profiles - getAuthentication groupcheck 'wifitest' domain
lab.wnam.ru groups: [Wi-Fi Test Users, DnsAdmins]
00.470 local-admins-profiles - getAuthentication groupcheck membership matched
user in group 'Wi-Fi Test Users'
00.470 local-admins-profiles - getAuthentication pcandidates left: 1
00.470 local-admins-profiles - getAuthentication profile 'CheckPoint Super'
00.470 local-admins-profiles - getAuthentication resulting profile is for
ACTIVE_DIRECTORY, password and groups are checked
00.470 filterForPapMacMethod - CheckLocalAdminProfiles user 'wifitest' matched,
state: OK_SKIP, admin profile: 'CheckPoint Super'
```

3. (, .) :

```
 Calling-Station-Id = "172.16.130.5"
 Cleartext-Password = "wifitest1"
Received Access-Reject Id 226 from 172.16.130.5:1812 to 172.16.130.13:48626
length 20
```

13.11.2023 01:39:15	00:00:00:00:00:00	172.16.130.5	wifitest	VPN Fake Site	checkpoint64 [R20 VM] 172.16.130.13	Default reject	no-pap-profiles-matched

:

```
00.097 local-admins-profiles - getAuthentication prio=42,
method=ACTIVE_DIRECTORY, pcandidate=CheckPoint Super
00.097 local-admins-profiles - getAuthentication checkInDomain lab.wnam.ru,
group_list=password check failed
00.097 local-admins-profiles - getAuthentication pcandidates left: 0
00.097 local-admins-profiles - profile matching, no candidates left, fail
00.097 trace - filterForPapMacMethod profile 'CheckPoint test',
pass_profile=false, identity_rule=LocalAdmin
00.097 filterForPapMacMethod - removed 'CheckPoint test', mismatch in identity
sources
```