

# 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:

Изменение сервера доступа

Параметры

RADIUS

SNMP

TACACS+

Порты

Категории

Подразделение

Сбер

Тип

Имя устройства

LAN Switch

checkpoint64

IP адрес (NAS-IP-Address)

Внешний IP адрес

172.16.130.13

192.168.1.1

Местоположение

R20 VM

Комментарий

Логин

Пароль

2. - (, )

3. ADCTool [lab.wnam.ru](http://lab.wnam.ru)

#### 4. RADIUS- (" - ") , :

### Правило аутентификации

Отменить Клонировать Удалить Сохранить

**Включено** ☒ Да

**Наименование** CheckPoint test

**Приоритет** 200

**Время** ☒ Любое ☐ Рабочие часы с:  по:

**Источник запроса**

☐ Любой

☐ Подразделение:

☒ Сервер доступа:

☐ Категории серверов доступа

☐ Совпадение в NAS Identity

☐ Проводный ☐ Беспроводной ☒ VPN ☒ Логин

**Источник проверки учётных данных**

☐ Не применимо

☐ Пароль в существующем эндпоинте

☐ Администратор WNAM

☒ Профили администраторов оборудования

☐ Служба каталога:

☐ Группа:

☐ Строка в имени группы:

☐ Совпадение в атрибуте службы каталога

☒ значение:  ☐ из RADIUS-атрибута:

**Эндпоинт** ☒ любой ☐ машинный ☐ предварительно машинно-авторизованный

**Метод**

Простая авторизация по MAC адресу (MAB) или паролю

☒ PAP

MAC адрес: ☐ Известен и валиден ☐ Не известен ☐ Просрочен/не валиден

Совпадение в MAC адресе

☐ Допустить ранее авторизованные 802.1X эндпоинты

**Результат**

☐ Deny (и проверить правила авторизации)

☒ Allow (и проверить правила авторизации)

☐ Redirect на гостевой портал авторизации

☐ FastAllow и назначить VLAN: ☒ нет ☐ IEEE ☐ HP  Номер

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

### Администратор или пользователь оборудования

Отмена Удалить

**Включено** ☒ Вкл. **TACACS+** ☒ Вкл. **RADIUS** ☒ Вкл.

**Логин** pupkin

**Полное имя** Vasily Pupkin

**Уровень доступа** 15

**Пароль** .....

**Повторите пароль** .....

6. (" - "):

## Группа администраторов

Отмена Удалить

Название Checkpoint monitor role

Администраторы pupkin (Vasily Pupkin)

Группы администраторов

- ☐ aaa1 ()
- ☐ aaaa (Vasya Pupkin)
- ☒ pupkin (Vasily Pupkin)
- ☐ test (test User)
- ☐ wifiastra (Wifi Astra User)
- ☐ wifitest2 (Testing Lastname)

Категории

7. , , (" - ").  
:

## Профиль администраторов

Отмена Удалить Сохранить

Включено ☒

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-Gala-SuperUser-Access	0
CP-Gala-User-Role	monitorRole

8. , - (: ). ):

Профиль администраторов

Отмена

Удалить

Сохранить

Включено

Вкл

Наименование

CheckPoint Super

Приоритет

42

Уровень привилегий

15

☒ не передавать

Источник подключения

☒ IP адрес/сеть

172.16.130.0/24

Протокол

☒ RADIUS ☐ TACACS+

Нижеследующие настройки совпадения по цели, пользователю (кроме "Локальный"), присваиваемые команды распространяются только на TACACS+ подключения.

Цель подключения

☐ Любой

☐ Подразделение

☒ Сервер доступа

- любой -

172.16.130.13 checkpoint64 R20 VM

Пользователь

☐ Администратор WNAM

☐ Строка в имени

☐ Локальный

Выбранные пользователи

wifitest2 (Testing Lastname)

Выбранные группы

GuestType\_Contractor (default), GuestType\_Daily (default)

☒ Из домена

Домен AD

lab.wnam.ru

☒ Группа AD

Wi-Fi Test Users

☐ Строка в имени группы

aa

☐ Список логинов

Выбор

Доступ

☒ Разрешен ☐ Запрещен

Атрибуты

Добавить атрибут

Имя	Значение
CP-Gaia-SuperUser-Access	1
CP-Gaia-User-Role	adminRole

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
```

"\_ " :

Параметры записи о сессии

MAC

00:00:00:00:00:00

Идентификатор

pupkin

IP адрес

172.16.130.5

SSID

Площадка

VPN Fake Site

Сервер доступа

checkpoint64 [R20 VM] [172.16.130.13]

Аутентификация

CheckPoint test

Авторизация

Admin Access

Время начала

13.11.2023 01:29:51

Имя

R

Vasiliy Pupkin

Метод

PAP

Фреймов

1

Тэг

✓

Тэг

✓

Лог подключения:

1: fillFromRadiusAttributes - identity: 'pupkin', portType: User

2: fillFromRadiusAttributes - mac: '00:00:00:00:00:00

3: fillFromRadiusAttributes - password: present in request, same as username

4: fillFromRadiusAttributes - nas: 'checkpoint64 [R20 VM]', id: 5fa3c7a5a2bad2116c59c4e2, vendor: LANSW [enabled]

5: fillFromRadiusAttributes - nas: IP address: 172.16.130.13, identifier: 'null', port: 'null'

6: fillFromRadiusAttributes - site: 'VPN Fake Site', id: 702 [enabled]

7: fillFromRadiusAttributes - session id: '1699828191707-172.16.130.13'

8: radius - received 5 attributes in the request:

User-Name = pupkin

Calling-Station-Id = 172.16.130.5

User-Password = pupkin

NAS-IP-Address = 172.16.130.13

```
00.015 filterForAlMethod - 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 - !!! WNAME 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'
```

```
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
```

"-":

Параметры записи о сессии

MAC

00:00:00:00:00:00

Время начала

13.11.2023 01:36:12

Идентификатор

wifitest

Имя

R

IP адрес

172.16.130.5

Метод

PAP

SSID

Фреймов

1

Площадка

VPN Fake Site

Сервер доступа

checkpoint64 [R20 VM] [172.16.130.13]

Аутентификация

CheckPoint test

Тэг

✓

Авторизация

Admin Access

Тэг

✓

Лог подключения:

1: fillFromRadiusAttributes - identity: 'wifitest', portType: User

2: fillFromRadiusAttributes - mac: '00:00:00:00:00:00

3: fillFromRadiusAttributes - password: present in request, same as username

4: fillFromRadiusAttributes - nas: 'checkpoint64 [R20 VM]', id: 5fa3c7a5a2bad2116c59c4e2, vendor: LANSW [enabled

5: fillFromRadiusAttributes - nas: IP address: 172.16.130.13, identifier: 'null', port: 'null'

6: fillFromRadiusAttributes - site: 'VPN Fake Site', id: 702 [enabled]

7: fillFromRadiusAttributes - session id: '1699828572348-172.16.130.13'

8: radius - received 5 attributes in the request:

User-Name = wifitest

Calling-Station-Id = 172.16.130.5

User-Password = wifitest

NAS-IP-Address = 172.16.130.13

NAS-Port-Type = Virtual

Детальный лог подключения

Заккрыть

,"

```
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

```