v1.14_ESR-10 OTT (1.6.0) .

-
  -
  -
-
  - - ESR-10
  - ELTEX-WIFI-SA
  - ISC-DHCP-SERVER
-
  - EMS
-
  - BRAS
  -
  - SSID
  - L2
  - OTT
  - ESR-10 OTT
    - 1) OTT ESR-10
    - 2) EMS OTT, , MAC- ,
-
  - OTT , -
    -
    - default OTT
    -
  - , ESR-10 -

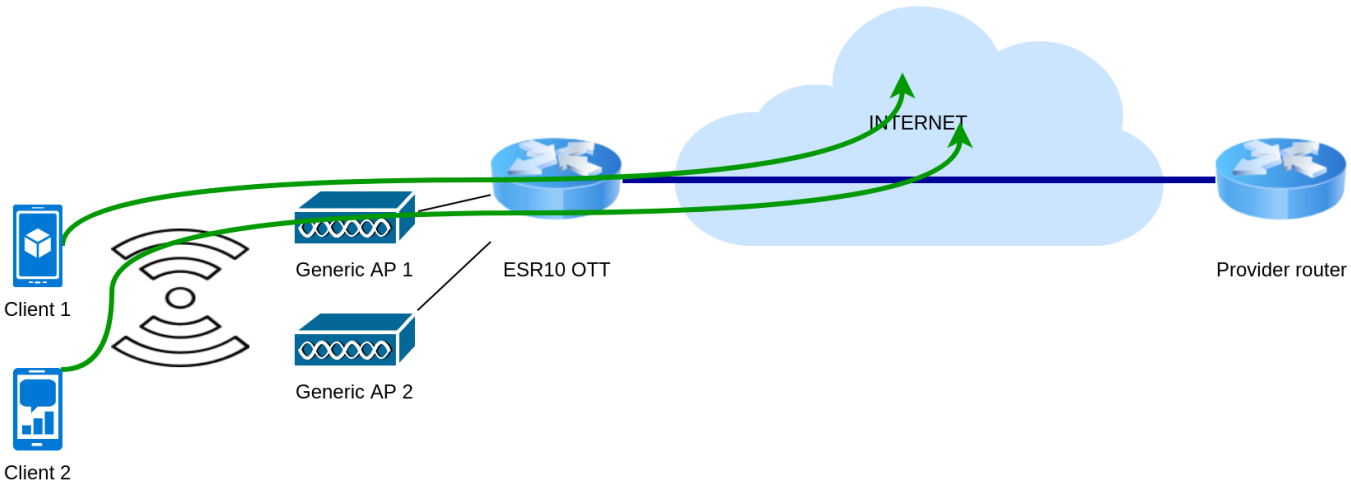
, SoftWLC OTT BRAS (,) .

GRE over IPsec ESR, OTT. .

, ESR-10, GRE over IPsec , ESR-10 .

"OTT " ESR-10 Jerry, v1.12_Jerry.

Общая схема подключения



managment traffic

data traffic

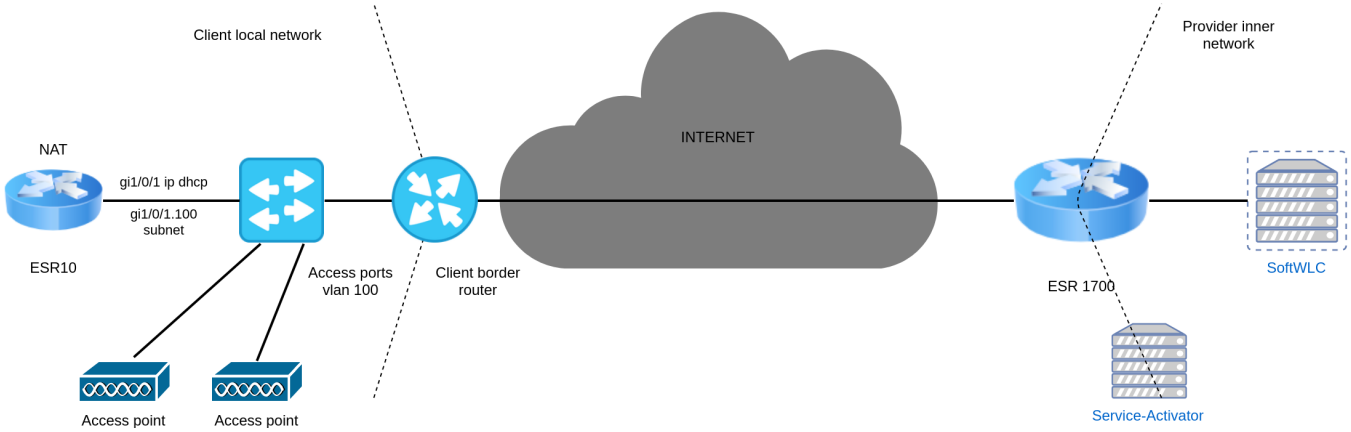
1) gi1/0/1 ESR10;

2) DHCP, default gateway DNS ;

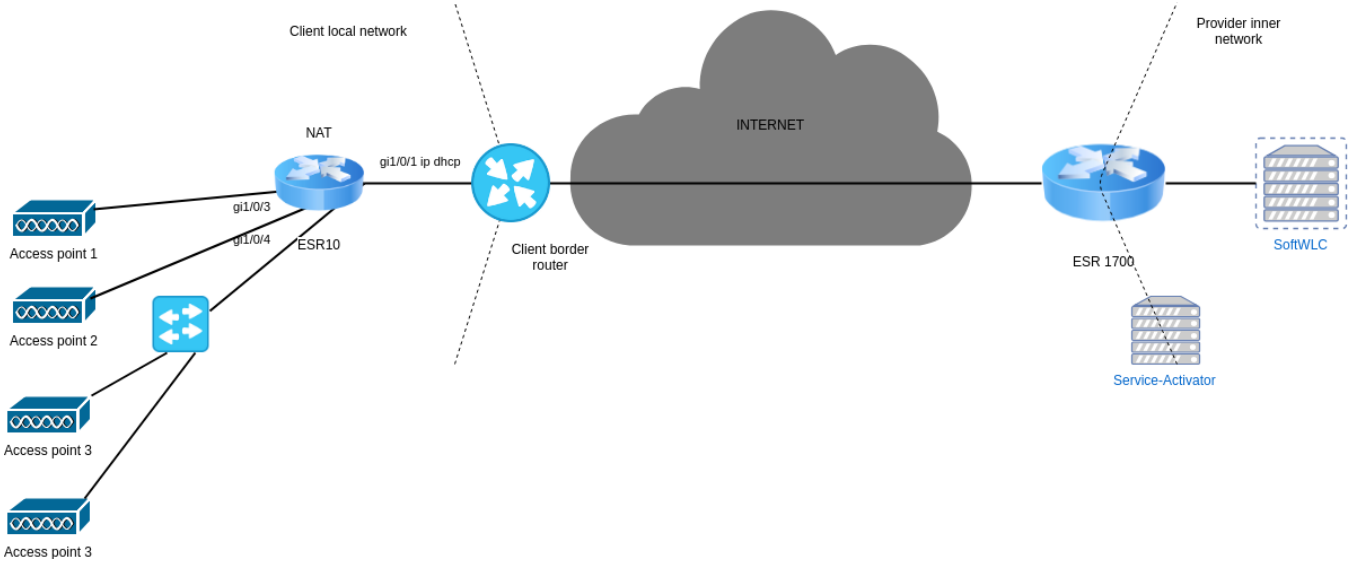
3) ESR10 .

BRAS ESR-10 L3, , , ESR 10 . NAT ESR10, routing, NAT .

1. ESR-10 . ESR10 , SSID, , - ESR-10. ESR-10, , NAT.



2. ESR-10 , . ESR10 , - . ESR10 NAT, .



ESR-10 OTT:

1) ESR-10 - ESR10 , , , , .

2) , (OTT) MAC- ESR-10, , SoftWLC (L2 ,) - ESR-10 .

- ESR-10

ESR-10 OTT, . - - factory-config. , , ("password", -):

```
esr-10(change-expired-password)# password password

esr-10(change-expired-password)# comm

Configuration has been successfully applied and saved to flash. Commit timer started, changes will be reverted in 600 seconds.

2019-02-07T12:15:53+00:00 %CLI-I-CRIT: user admin from console  input: commit

esr-10(change-expired-password)# confirm

Configuration has been confirmed. Commit timer canceled.

2019-02-07T12:15:57+00:00 %CLI-I-CRIT: user admin from console  input: confirm

esr-10#
```

debug -:

```
esr-10# debug

esr-10(debug)# service-activator url https://sa.example.org:8043
```

- / DHCP url .

OTT - url -:

```
esr-10(debug)# no service-activator url

esr-10(debug)# show service-activator url

esr-10(debug)#
```

- ESR-10.

ELTEX-WIFI-SA

/var/lib/eltex-wifi-sa/firmware/

```
root@softwlc-ott:/tftpboot# mv -v /tftpboot/esr1x-1.6.0-build3.firmware  /var/lib/eltex-wifi-sa/firmware/

‘/tftpboot/esr1x-1.6.0-build3.firmware’ -> ‘ /var/lib/eltex-wifi-sa/firmware/esr1x-1.6.0-build3.firmware’
removed ‘/tftpboot/esr1x-1.6.0-build3.firmware’
```

/etc/eltex-wifi-sa/factory-fw.conf ESR10:

```
"ESR-10" {
min = 1.6.0.3
file = esr1x-1.6.0-build3.firmware
}
```

:

```
root@softwlc-ott:/tftpboot# service eltex-wifi-sa restart
eltex-wifi-sa stop/waiting
eltex-wifi-sa start/running, process 29739
```

ISC-DHCP-SERVER

ESR-10, OTT 43 15 , GRE keepalive. , OTT . , SoftWLC 121 .

, GRE keepalive , 172.16.27.1:

```
0F:0B:31:37:32:2e:31:36:2e:32:37:2e:31
```

.. ESR10 OTT GRE over IPsec , , 43- 15 10 , SNMP :

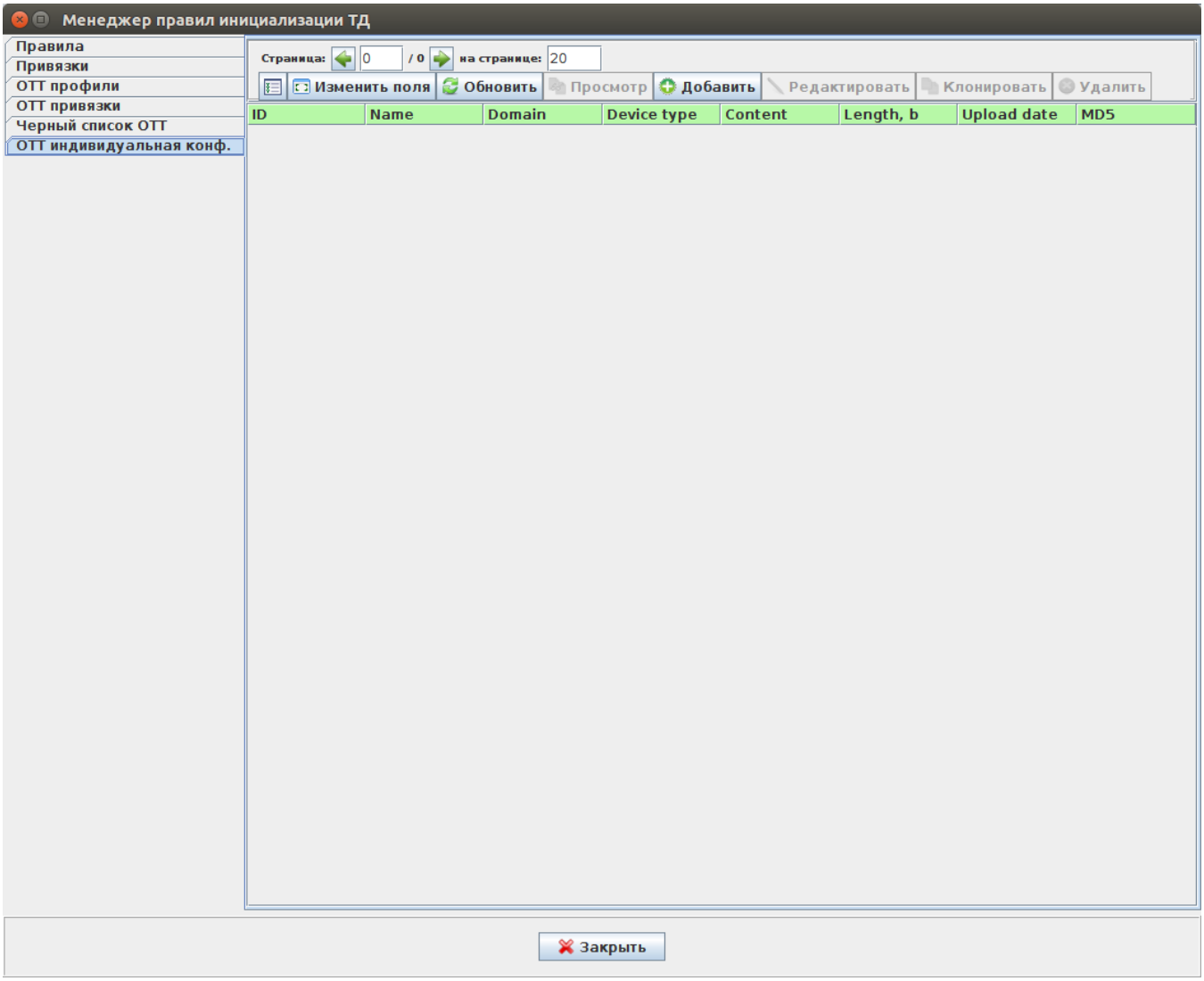
```
subnet 172.16.27.0 netmask 255.255.255.0 {
 pool {
  option routers 172.16.27.1;
  range 172.16.27.2 172.16.27.254;
  option vendor-encapsulated-options 0A:0E:31:39:32:2e:31:36:38:2e:34:32:2e:31:37:38:0f:0b:31:37:32:2e:31:36:2e:32:37:2e:31;
  option ms-classless-static-routes 24, 192,168,42, 172,16,27,1;
  option rfc3442-classless-static-routes 24, 192,168,42, 172,16,27,1;
  option ntp-servers 192.168.42.178;
  allow members of "ELTEX-DEVICES";
 }
}
```

ESR-10 , , . allow members of "ELTEX-DEVICES";

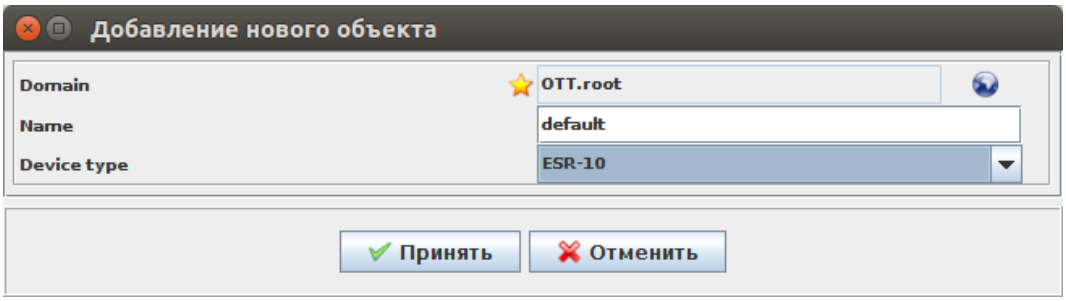
ESR "OTT .", , ESR-10 .

EMS

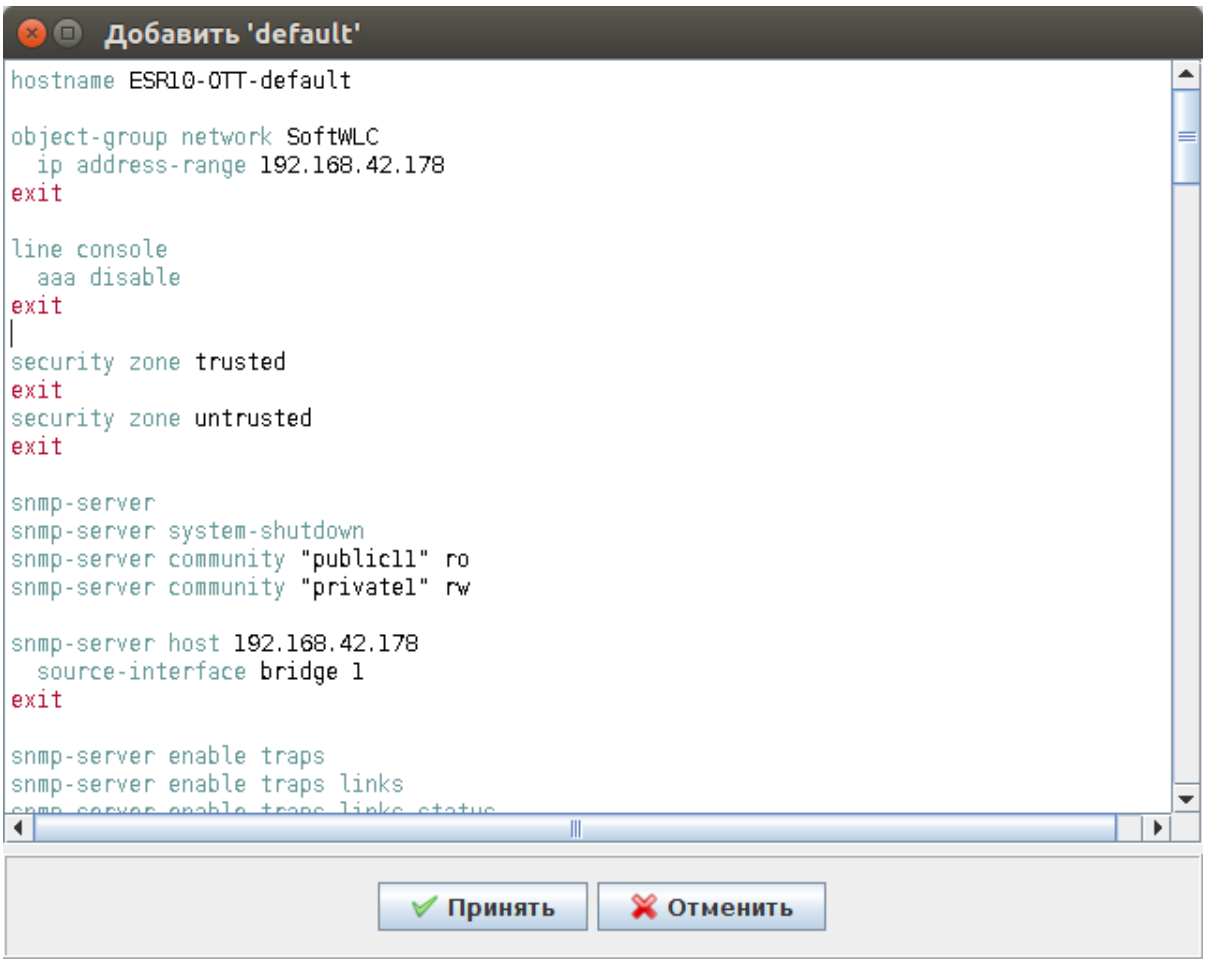
1. "Wireless" " ", "OTT ." "".



2. , - "default" (, ,), "device type" ESR-10 "".



3. "".



ESR10:

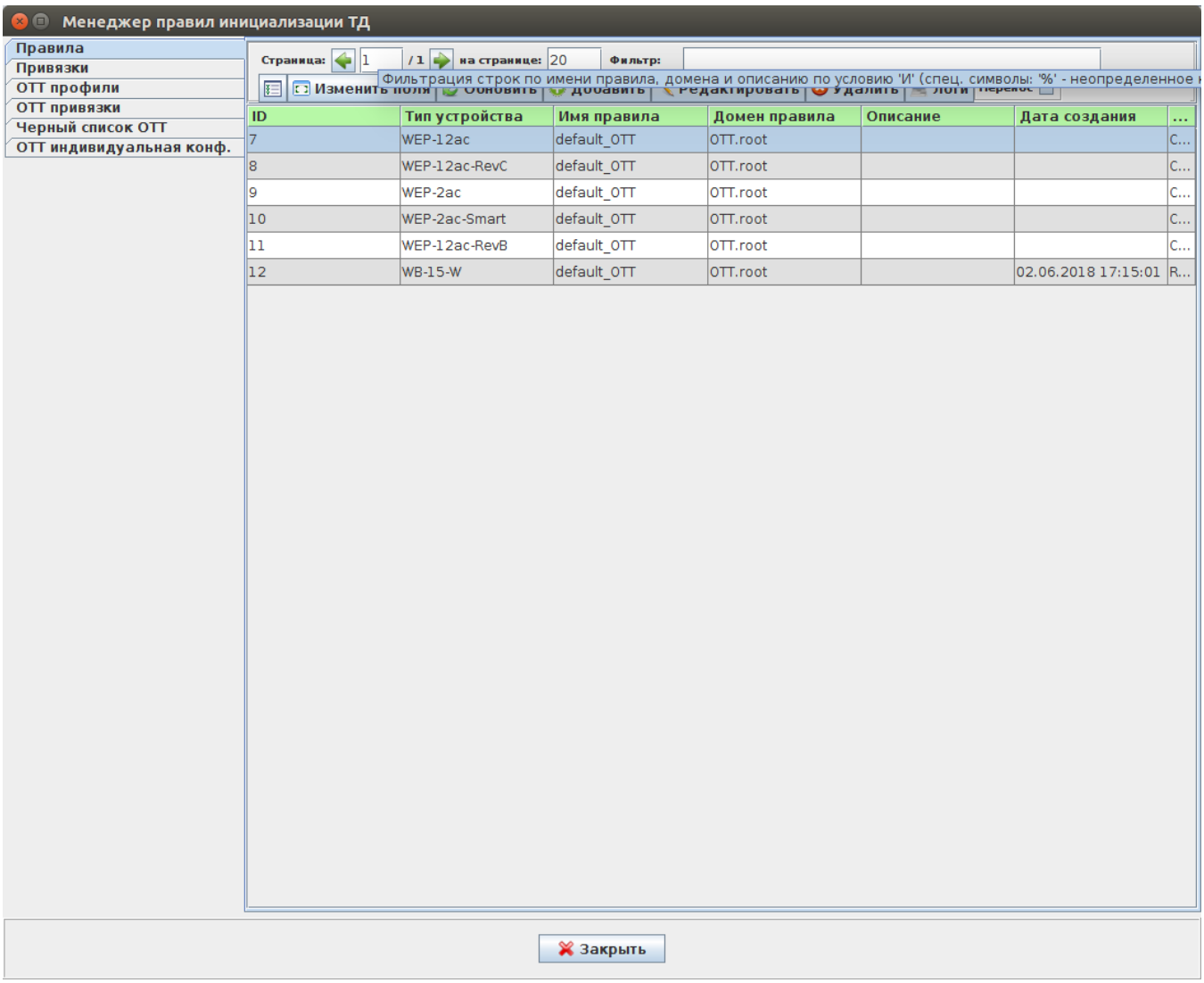
```
hostname ESR10-OTT-default

object-group network SoftWLC
 ip address-range 192.168.42.178
exit

line console
 aaa disable
exit

security zone trusted
exit
security zone untrusted
exit

snmp-server
snmp-server system-shutdown
snmp-server community "public11" ro
snmp-server community "private1" rw
```

```
snmp-server host 192.168.42.178
  source-interface bridge 1
exit

snmp-server enable traps
snmp-server enable traps config
snmp-server enable traps config commit
snmp-server enable traps config confirm
snmp-server enable traps environment
snmp-server enable traps environment memory-flash-critical-low
snmp-server enable traps environment memory-flash-low
snmp-server enable traps environment memory-ram-critical-low
snmp-server enable traps environment memory-ram-low
snmp-server enable traps environment cpu-load
snmp-server enable traps environment cpu-critical-temp
snmp-server enable traps environment cpu-overheat-temp
snmp-server enable traps environment cpu-supercooling-temp
snmp-server enable traps file-operations
snmp-server enable traps file-operations successful
snmp-server enable traps file-operations failed
snmp-server enable traps file-operations canceled
snmp-server enable traps interfaces
snmp-server enable traps interfaces rx-utilization-high
snmp-server enable traps interfaces tx-utilization-high
snmp-server enable traps interfaces number-high
snmp-server enable traps screen
snmp-server enable traps screen dest-limit
snmp-server enable traps screen source-limit
snmp-server enable traps screen icmp-threshold
snmp-server enable traps screen udp-threshold
snmp-server enable traps screen syn-flood
snmp-server enable traps screen land
snmp-server enable traps screen winnuke
snmp-server enable traps screen icmp-frag
snmp-server enable traps screen udp-frag
snmp-server enable traps screen icmp-large
snmp-server enable traps screen syn-frag
snmp-server enable traps screen unknown-proto
snmp-server enable traps screen ip-frag
snmp-server enable traps screen port-scan
snmp-server enable traps screen ip-sweep
snmp-server enable traps screen syn-fin
snmp-server enable traps screen fin-no-ack
snmp-server enable traps screen no-flag
snmp-server enable traps screen spoofing
snmp-server enable traps screen reserved
snmp-server enable traps screen quench
snmp-server enable traps screen echo-request
snmp-server enable traps screen time-exceeded
snmp-server enable traps screen unreachable
snmp-server enable traps screen tcp-all-flags
snmp-server enable traps entity
snmp-server enable traps entity config-change
snmp-server enable traps entity-sensor
snmp-server enable traps entity-sensor threshold
snmp-server enable traps envmon
snmp-server enable traps envmon shutdown
snmp-server enable traps envmon temperature
snmp-server enable traps flash
snmp-server enable traps flash insertion
snmp-server enable traps flash removal
snmp-server enable traps snmp
snmp-server enable traps snmp authentication
snmp-server enable traps snmp coldstart
snmp-server enable traps snmp linkdown
snmp-server enable traps snmp linkup
snmp-server enable traps syslog

bridge 1
  security-zone trusted
  ip address dhcp
  ip dhcp client ignore dns-nameserver
  ip dhcp client ignore router
  enable
exit
```

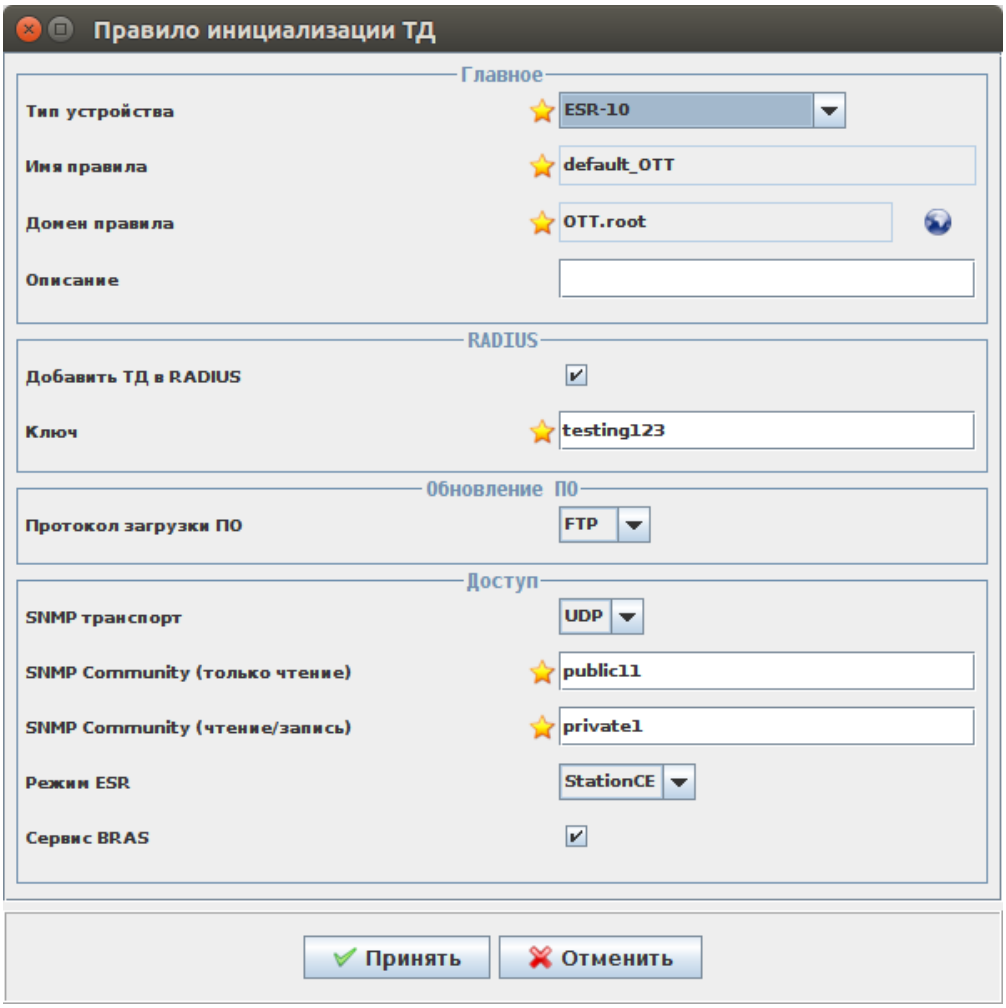
```
interface gigabitethernet 1/0/1
  description "UPLink"
  ip address dhcp
  security-zone untrusted
exit
interface gigabitethernet 1/0/2
  shutdown
exit
interface gigabitethernet 1/0/3
  shutdown
exit
interface gigabitethernet 1/0/4
  shutdown
exit
interface gigabitethernet 1/0/5
  shutdown
exit
interface gigabitethernet 1/0/6
  shutdown
exit
interface loopback 1
exit
tunnel gre 1
  keepalive dhcp dependent-interface bridge 1
  keepalive dhcp dependent-interface gi1/0/1
  mode ethernet
  local address xauth ipsec_vpn
  remote address xauth ipsec_vpn management-ip
  enable
exit
tunnel gre 1.1
  bridge-group 1
  snmp init-trap
  enable
exit

security zone-pair untrusted self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair trusted self
   rule 1
    action permit
    match source-address SoftWLC
    enable
  exit
exit

access profile acc_p
exit

security ike proposal ike_prop
exit

security ike policy ike_pol
  authentication method xauth-psk-key
  authentication mode client
  proposal ike_prop
exit

security ike gateway ike_gw
  ike-policy ike_pol
  assign-interface loopback 1
  local interface gigabitethernet 1/0/1
  remote network dynamic client
  mode policy-based
  dead-peer-detection action restart
  dead-peer-detection interval 10
exit

security ipsec proposal ipsec_prop
exit

security ipsec policy ipsec_pol
  proposal ipsec_prop
exit
```

```
security ipsec vpn ipsec_vpn
  mode ike
  ike establish-tunnel immediate
  ike gateway ike_gw
  ike ipsec-policy ipsec_pol
  enable
exit

ip ssh server
```

4. " " "" "":



5. :



:

1) " " - "ESR-10";

2) " " - "default_OTT" (, OTT , OTT);

3) " RADIUS" - ;

4) "" - "testing123";

5) " " - "FTP";

6) "SNMP " - "UDP";

7) "SNMP Community ( )" - "public11" (ESR - 8);

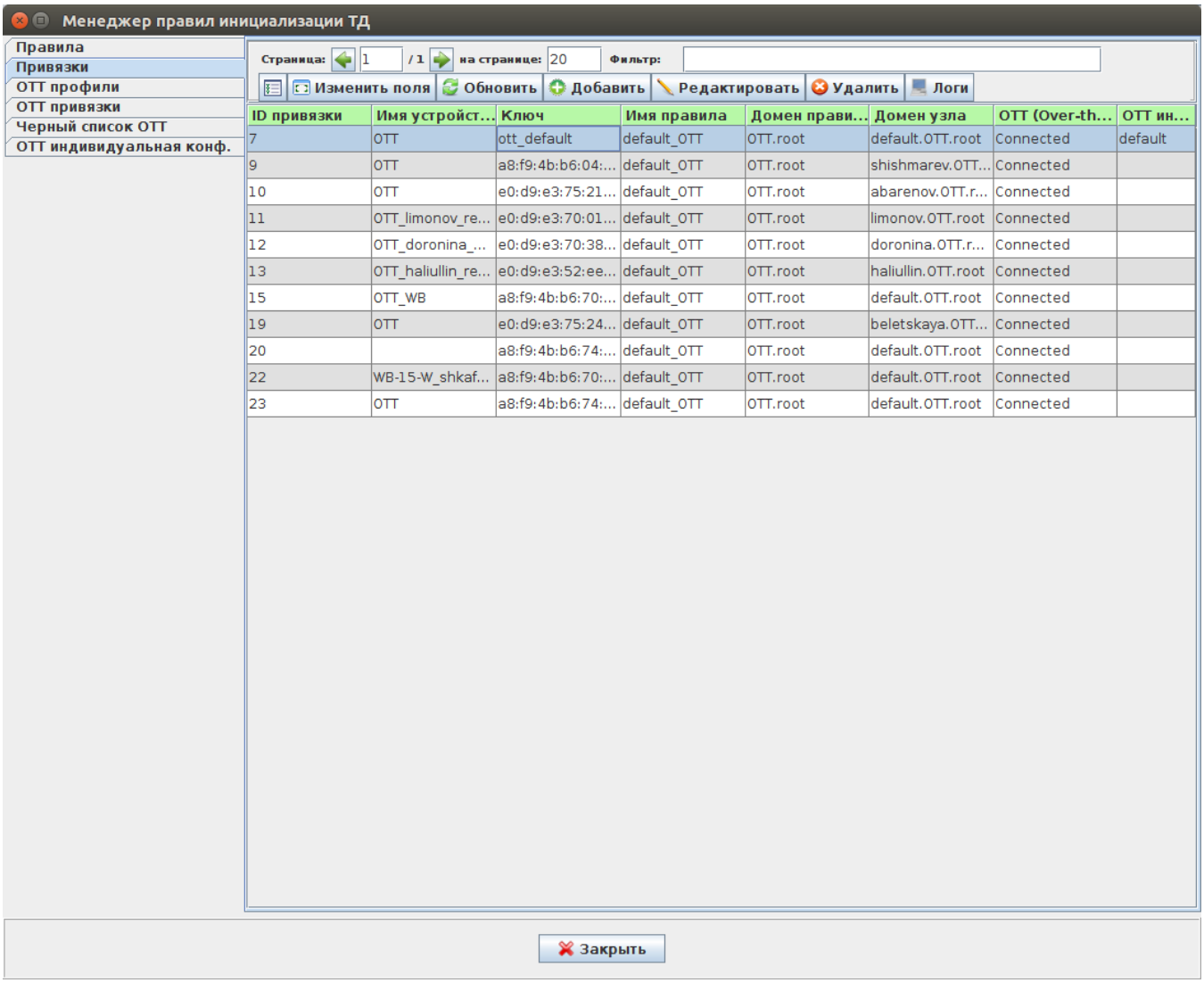
8) "SNMP Community (/)" - "private1";

9) ESR - "StationCE" (, , PCRF /);

10) " BRAS" - (ESR10 OTT , , OTT).

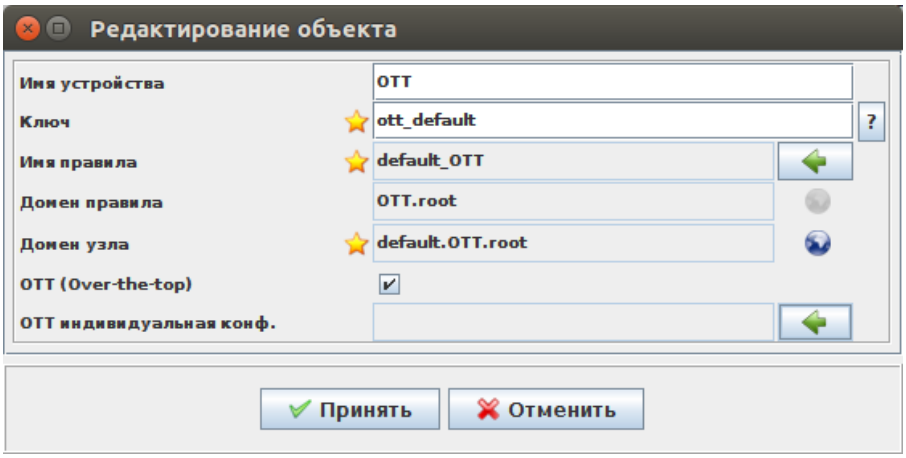
"".

6. " " "" OTT (, , OTT):

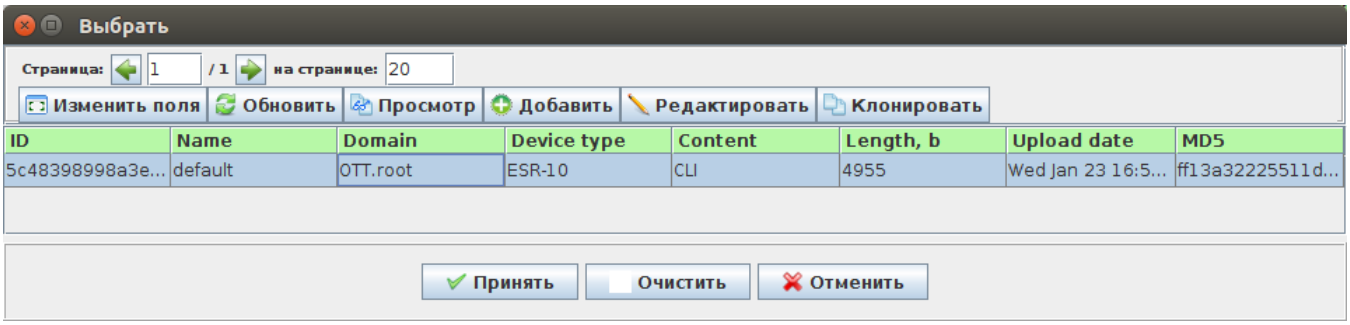


"".

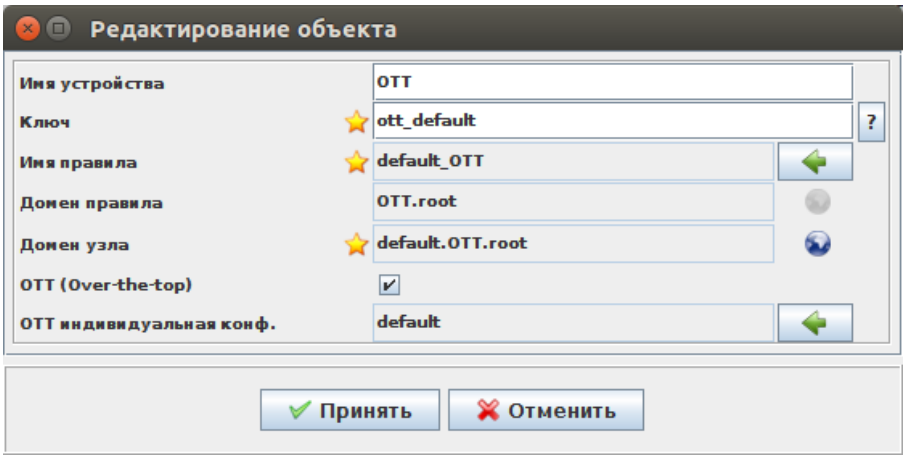
7. , "OTT .", ESR10 SA.



8. "default" "".



9. :



"".

10. " ". . ESR-10 , ,

- , :

1) (gi1/0/1) ESR10;

2) - gi1/0/2 - gi1/0/6;

3) , ( ) gi1/0/2-gi1/0/6 ESR-10.

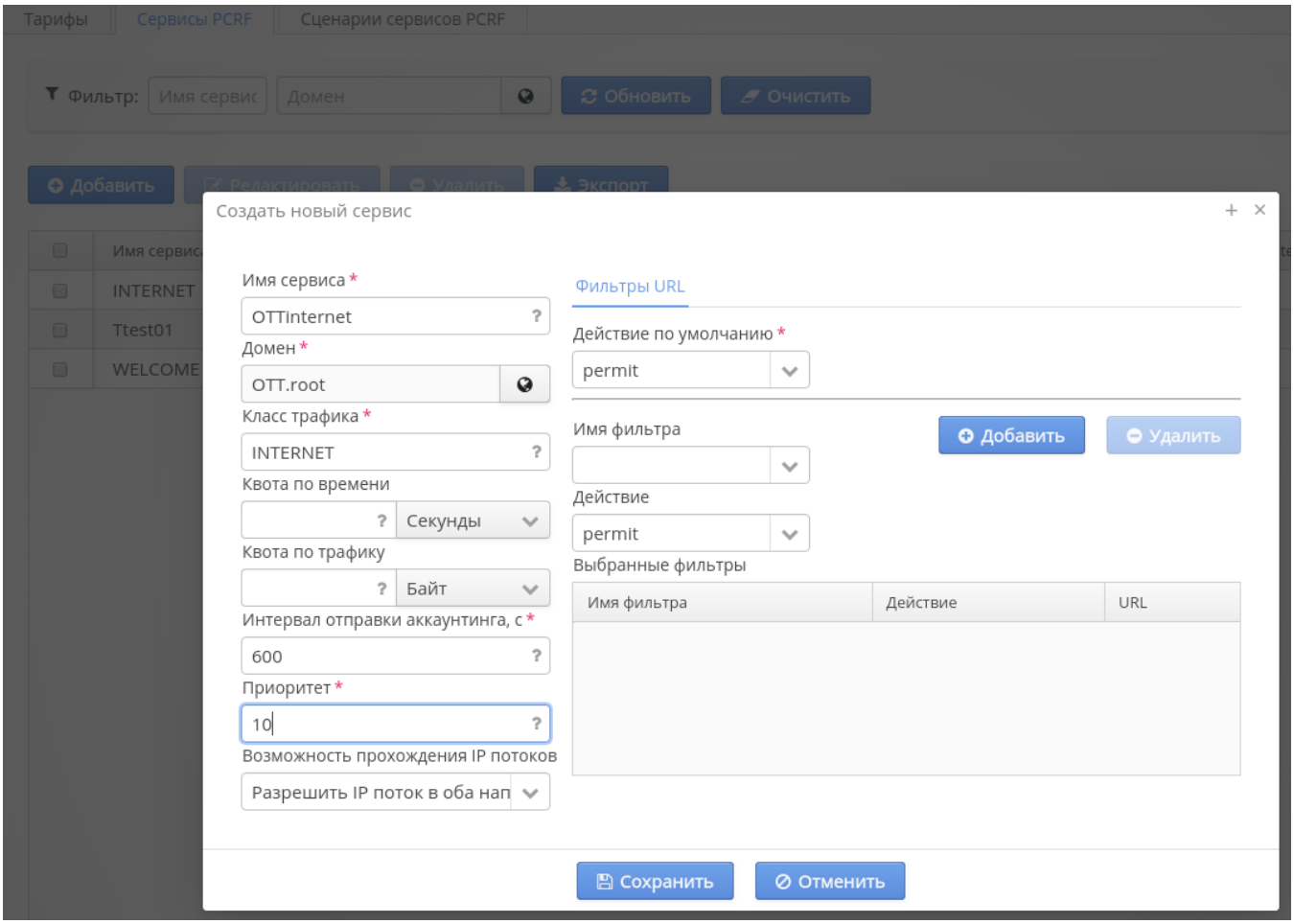
, MAC ESR-10, . , , ESR-10, , , , .

, ESR-10 , SSID, - SSID1 VID 701 SSID2 VID 702, location SSID12.

BRAS

BRAS. . , c OTT, WELCOME .

1. , " " " PCRF" "":



1) " " - "OTTinternet";

2) "" - ;

3) " " - "INTERNET";

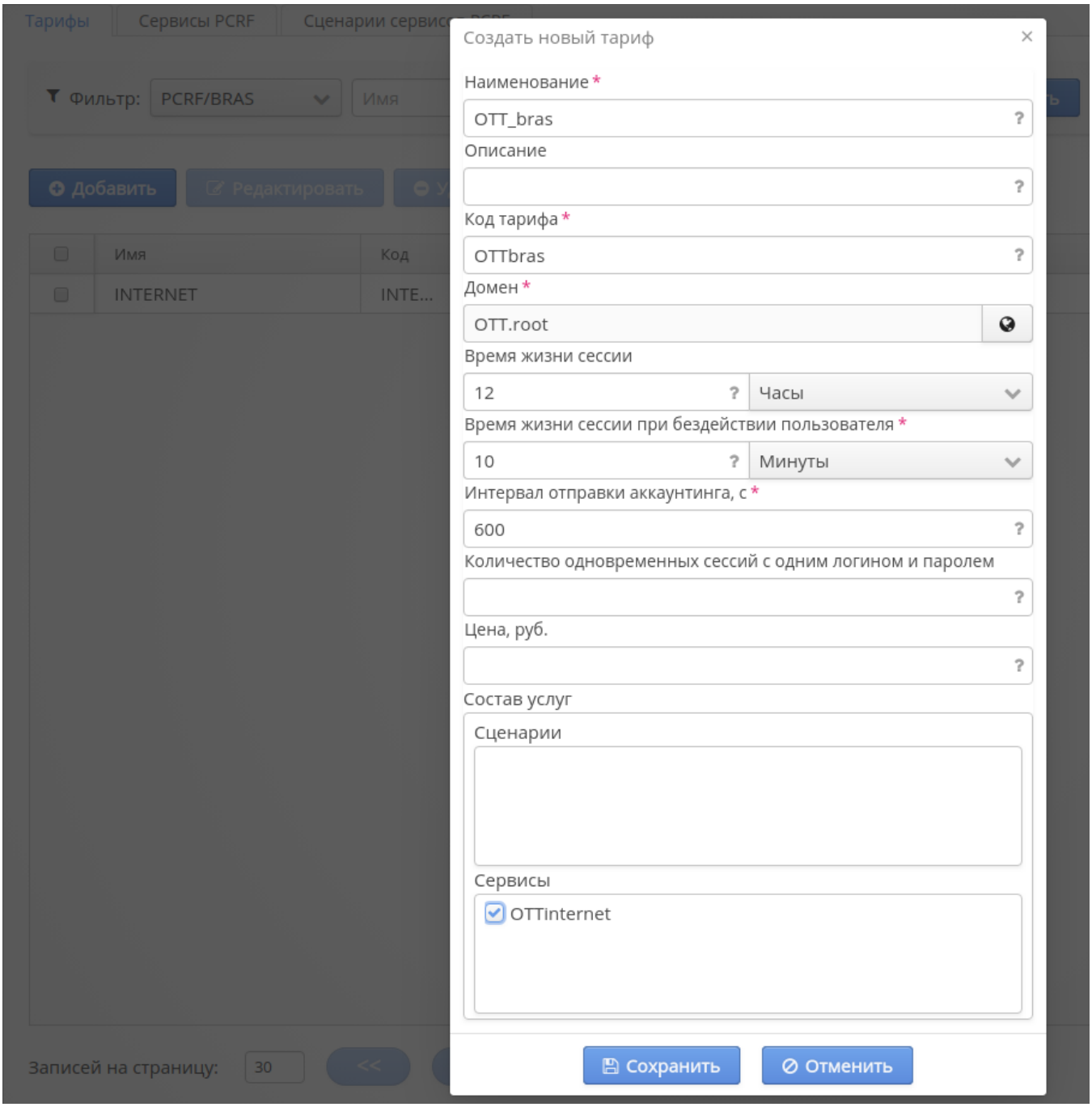
4) " " - "600";

5) "" - "10";

6) " IP " - " IP   ".

 "".

2. " PCRF" "", "PCRF/BRAS" "":



1) "" - ;

2) " " - ;

3) "" - (,);

4) " " - "12" ;

5) " " - "10" ;

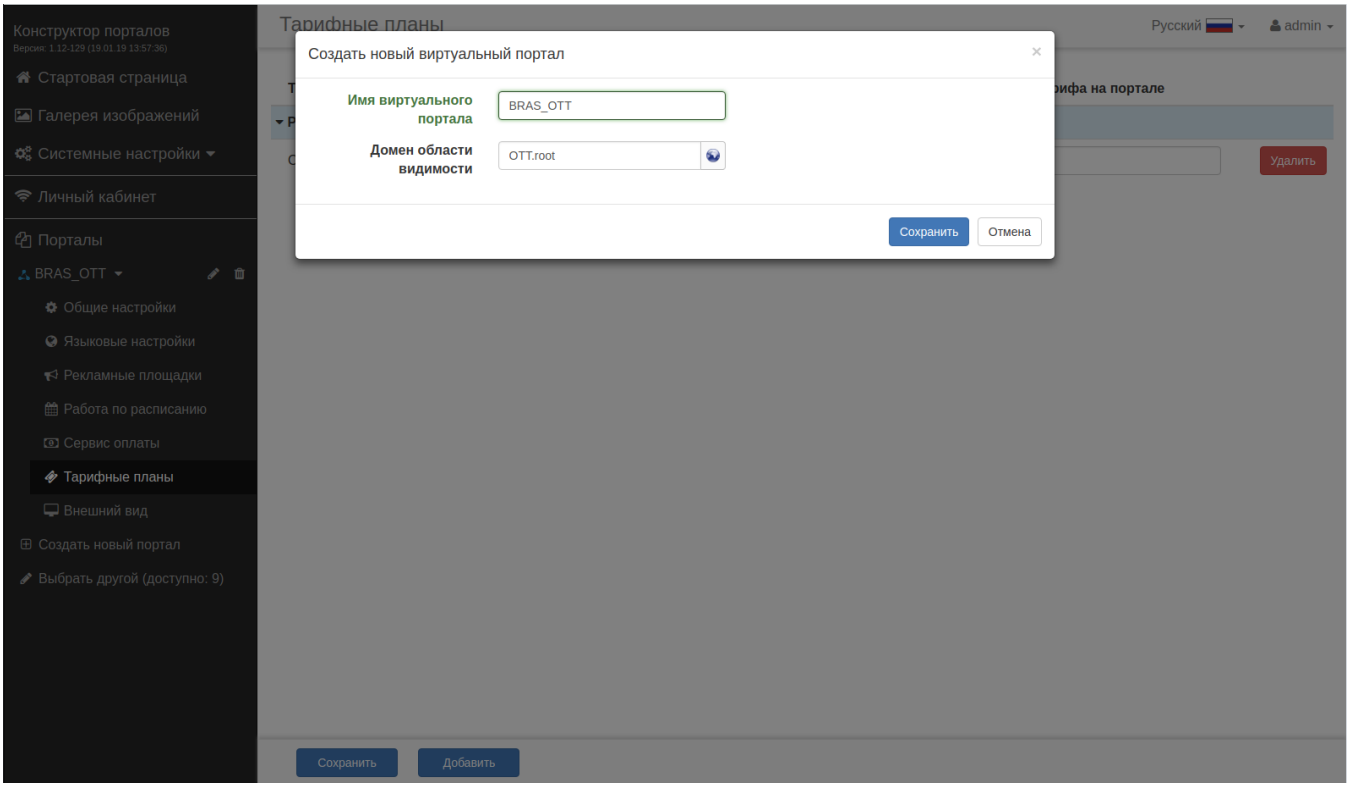
6) " " - "600" ;

7) "" - "OTTinternet";

"".

, BRAS. . . , BRAS .

1. , " ":

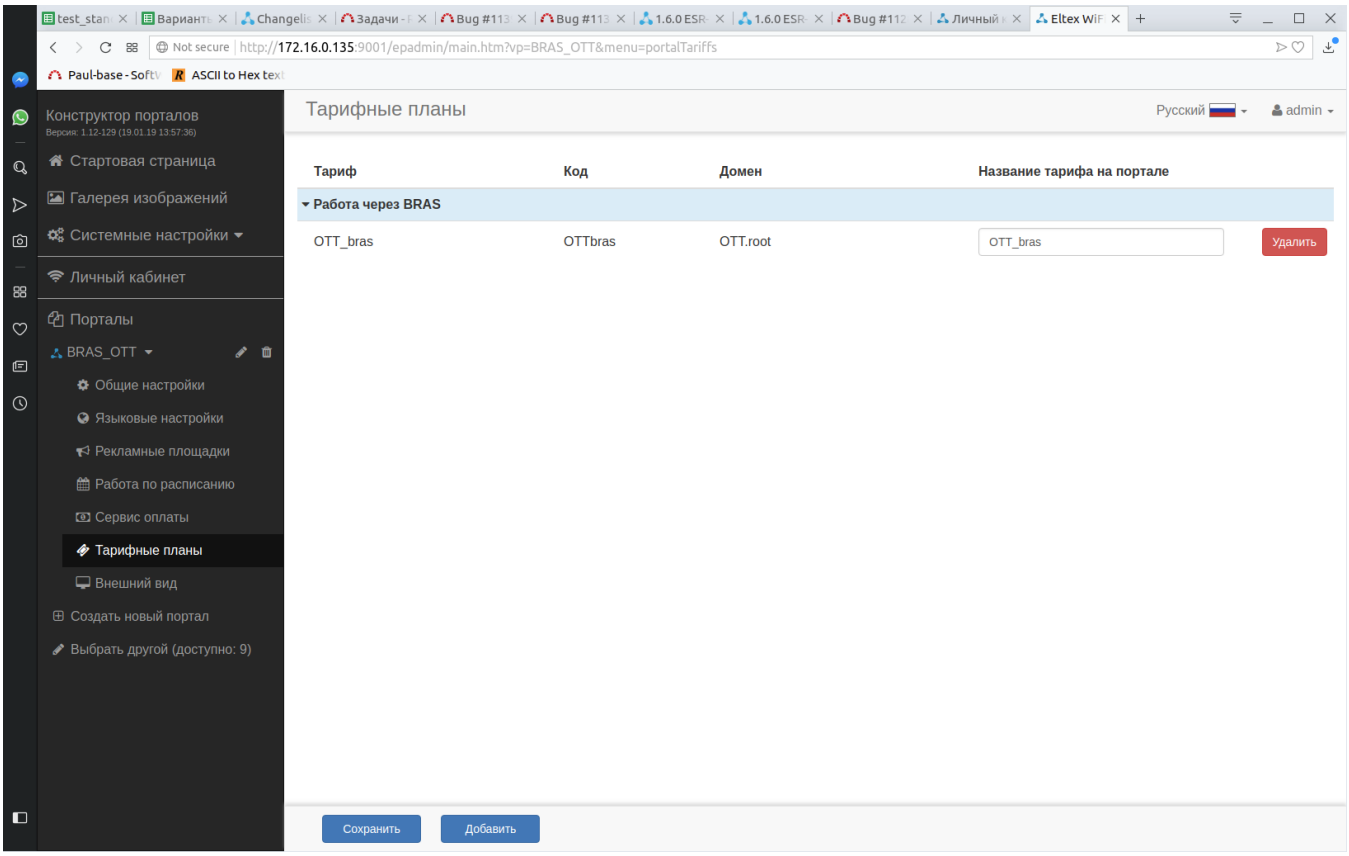


1) " " - ;

2) " " - ;

"".

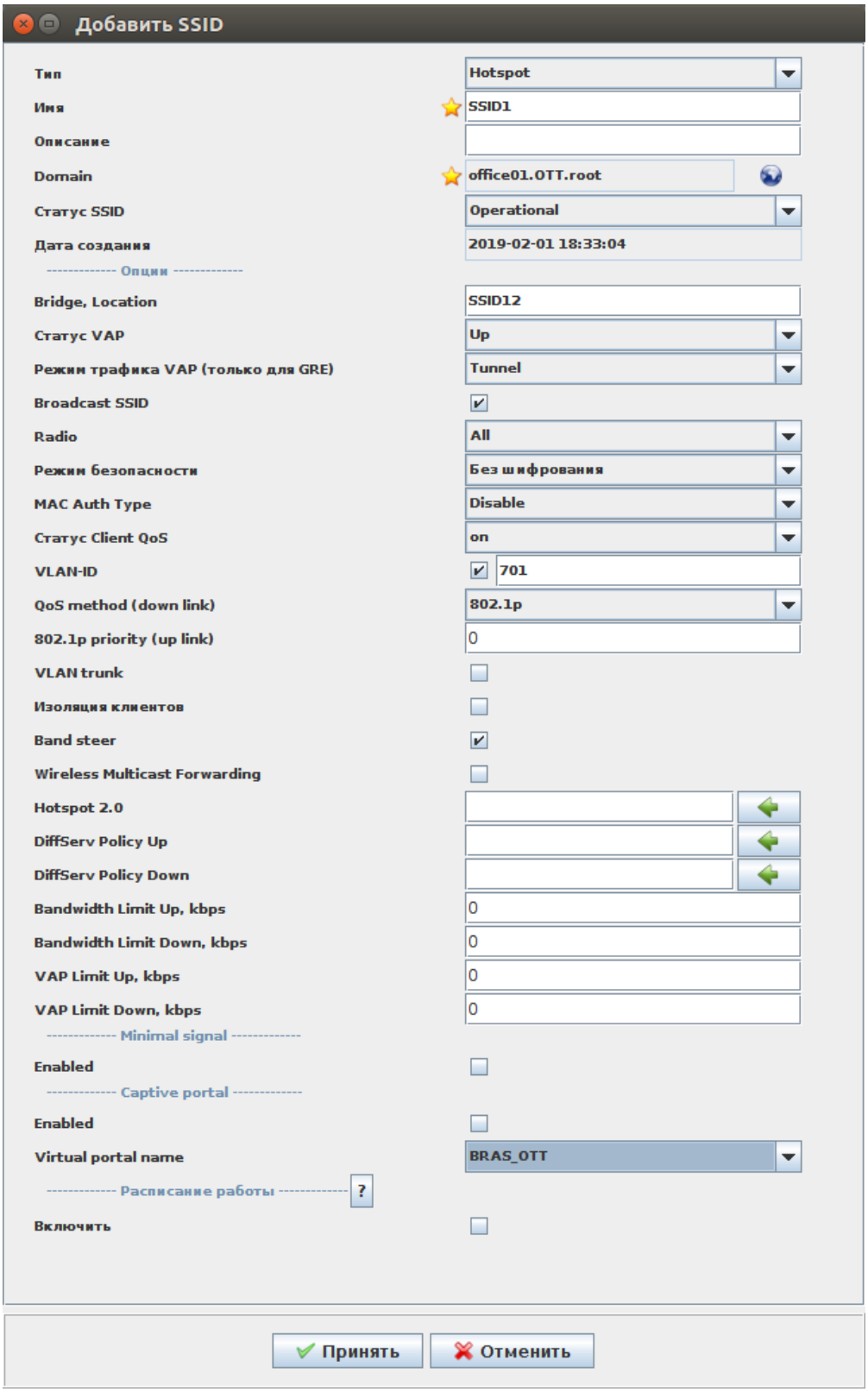
2. " " "OTT_bras":



"".

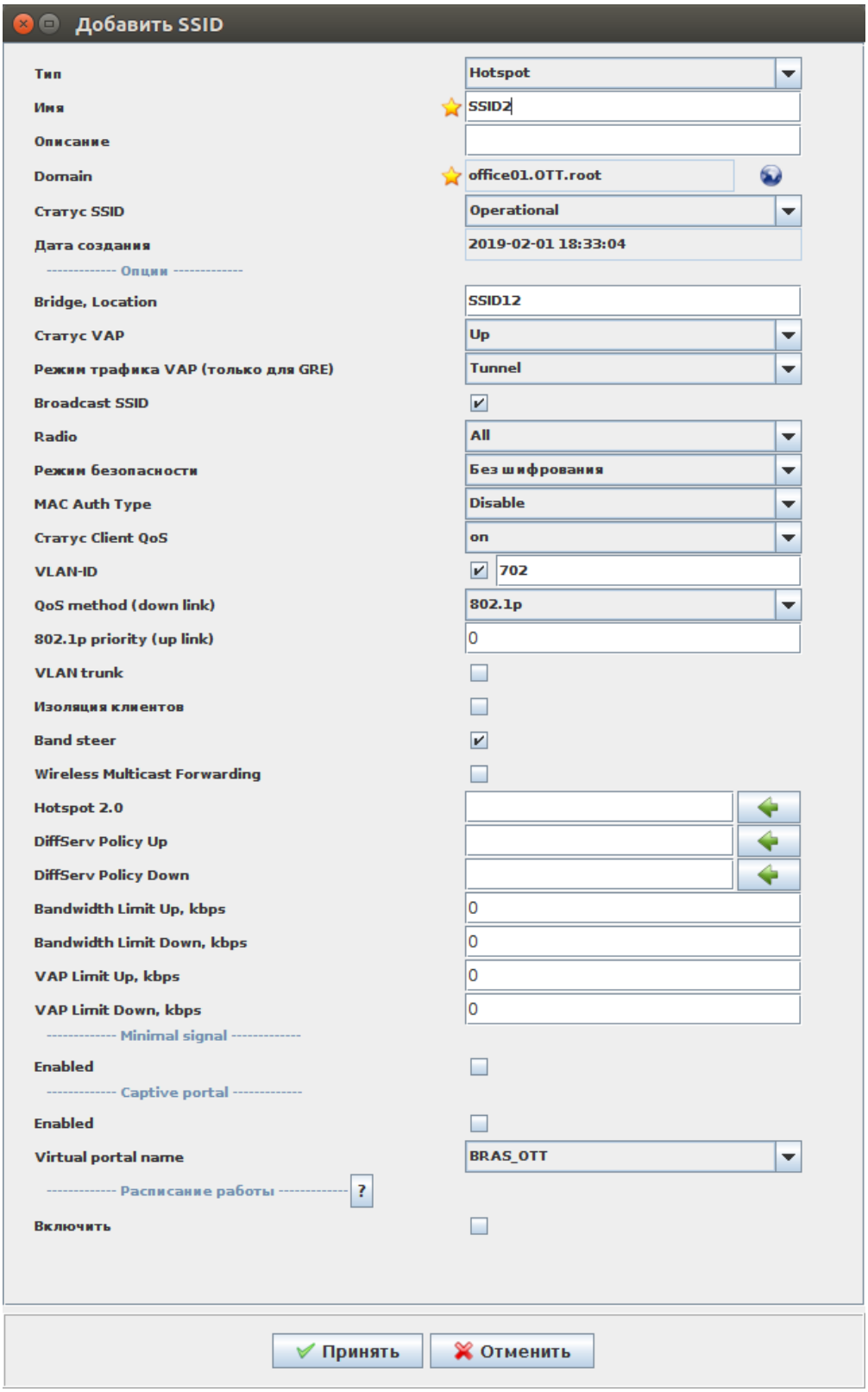
SSID

SSID , BRAS: "Wireless" " SSID" " SSID":



SSID1.

" VAP" "tunnel" - ESR-10 BRAS (SSID).



SSID2.

, ESR-10.

L2

L2 " ". . . IP- DHCP, . L2 OTT (BRAS ESR10) - "MAC, ". , L2 NAS MAC. NAS IP :

1) (SNMP ESR-10 MAC);

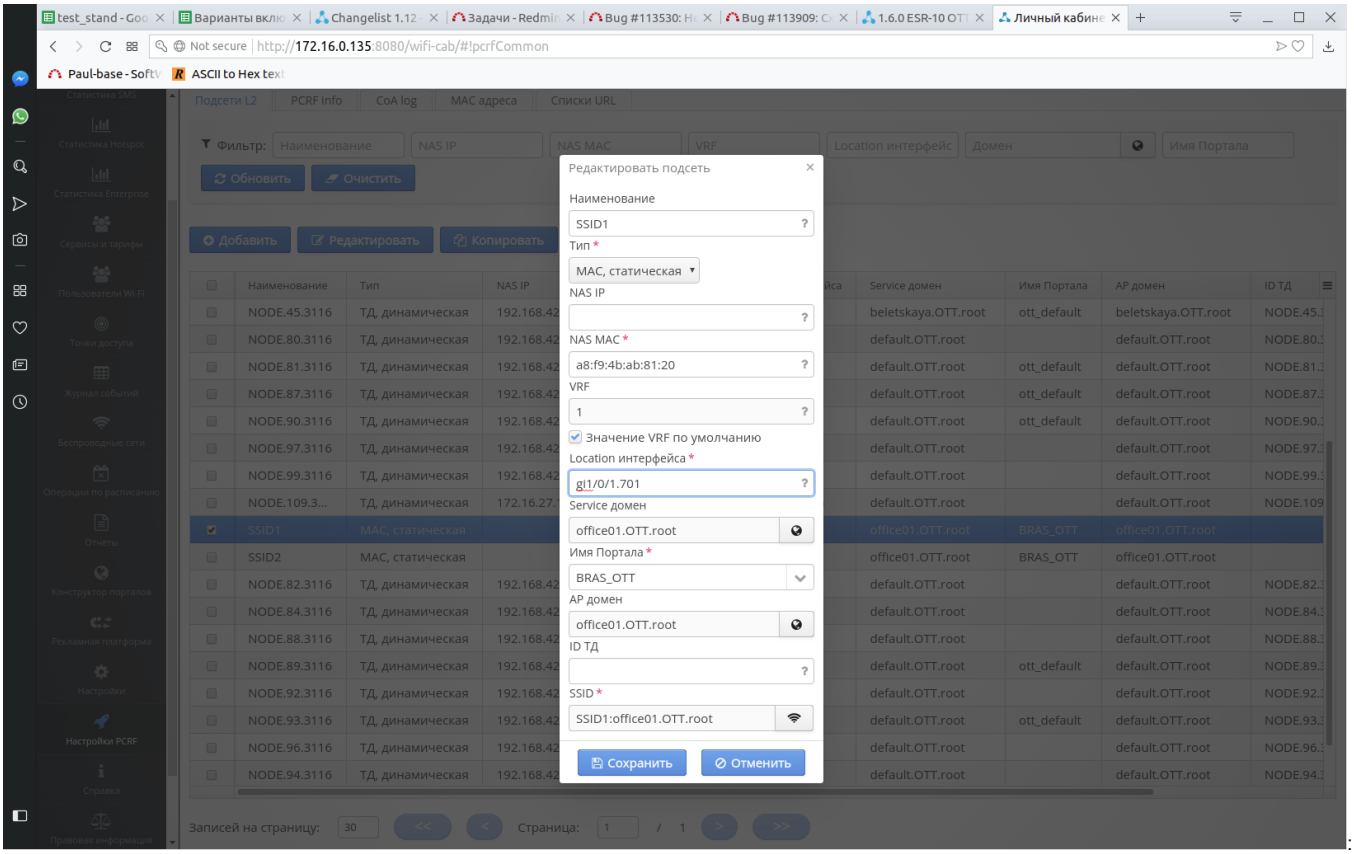
2) ;

3) .

"Notify PCRF about IP changed for MAC-based subnets".

L2 - SSID1 SSID2.

" PCRF" " L2" "":



:

 - "SSID1";

1) "NAS IP" - (IP);

2) "" - "MAC, ", MAC- ESR10;

3) "VRF" - " VRF ";

4) "Location" - location gi1/0/1.701 (-, SSID1);

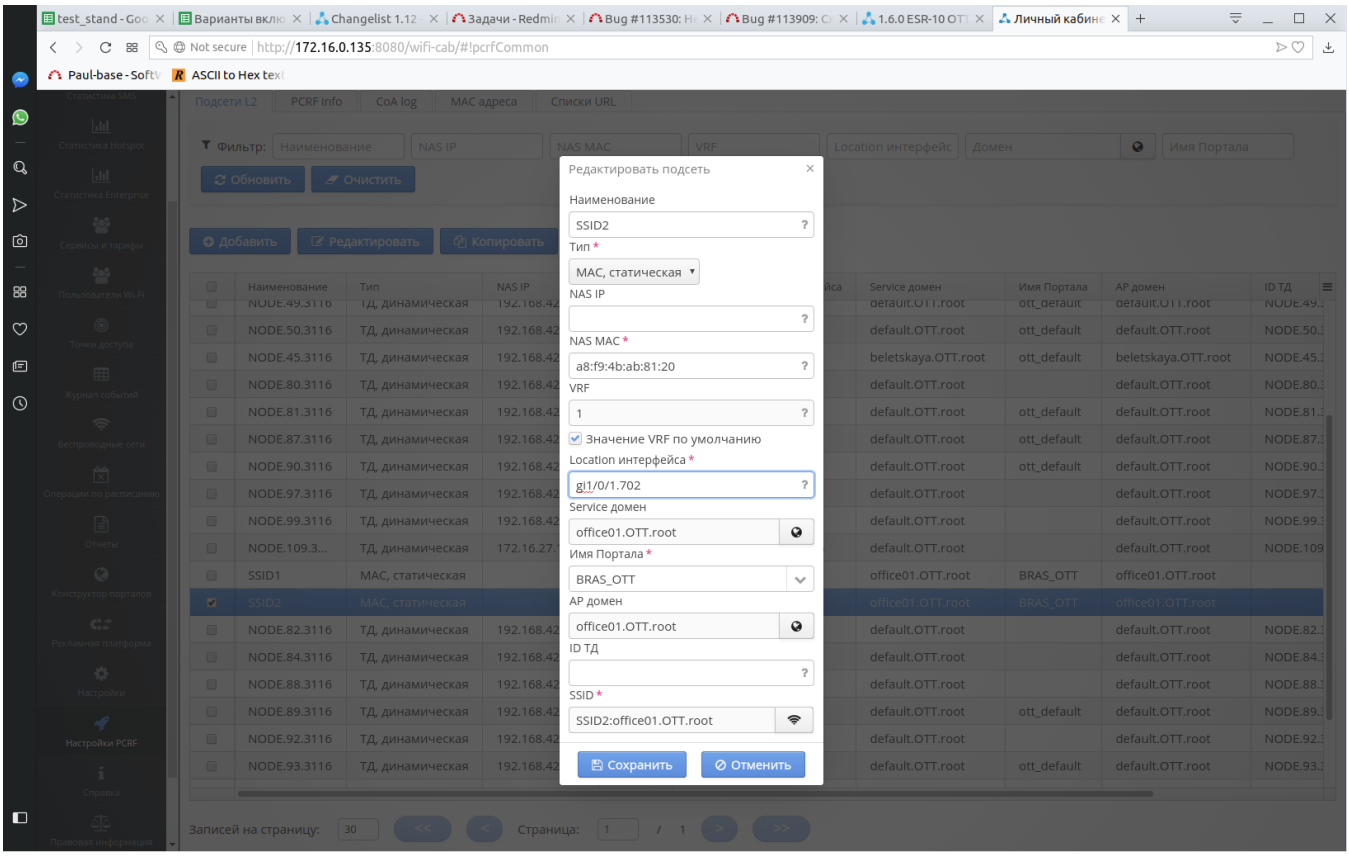
5) "Service " - SSID;

6) "AP " - ESR-10;

7) "SSID" - SSID (SSID1);

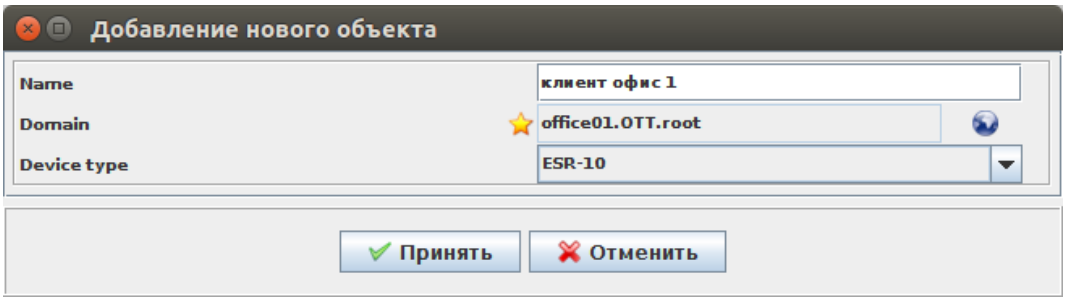
 "".

L2 SSID2:



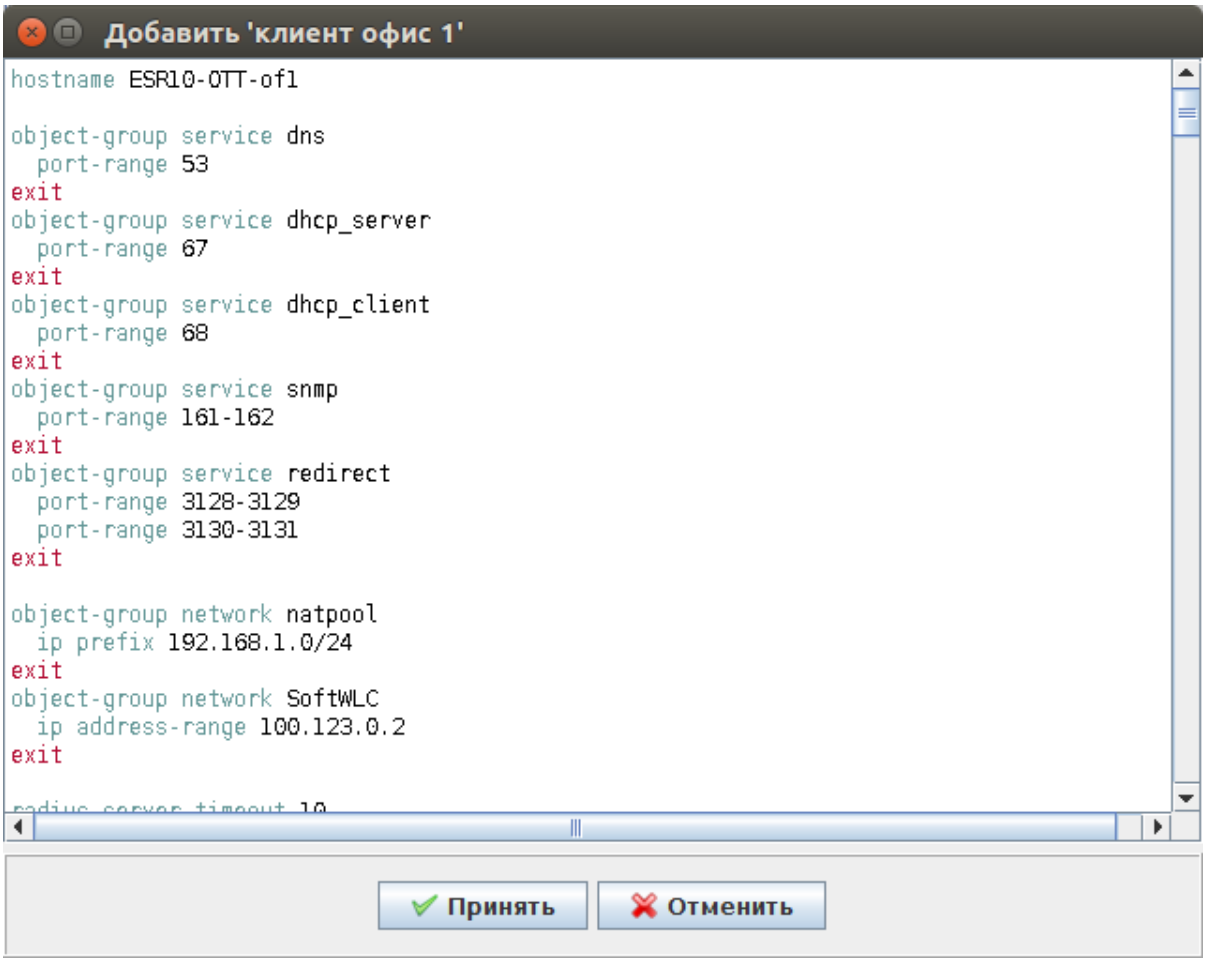
OTT

1. " ", "OTT ." :



, , Device type "ESR-10", "".

2. :




```
hostname ESR10-OTT-of1

object-group service dns
  port-range 53
exit
object-group service dhcp_server
  port-range 67
exit
object-group service dhcp_client
  port-range 68
exit
object-group service snmp
  port-range 161-162
exit
object-group service redirect
  port-range 3128-3129
  port-range 3130-3131
exit

object-group network natpool
  ip prefix 192.168.1.0/24
exit
object-group network SoftWLC
  ip address-range 192.168.42.178
exit
```

```
radius-server timeout 10
radius-server retransmit 5
radius-server host 192.168.42.178
  key ascii-text encrypted 88B11079B9014FAAF7B9
  timeout 11
  priority 20
  source-interface bridge 1
  auth-port 31812
  acct-port 31813
  retransmit 10
   dead-interval 10
exit
aaa radius-profile PCRF
  radius-server host 192.168.42.178
exit
das-server COA
  key ascii-text encrypted 88B11079B9014FAAF7B9
  port 3799
  clients object-group SoftWLC
exit
aaa das-profile COA
  das-server COA
exit
line console
  aaa disable
exit

domain lookup enable

security zone trusted
exit
security zone untrusted
exit
security zone user
exit

ip access-list extended WELCOME
  rule 1
    action permit
    match protocol tcp
    match destination-port 443
    enable
  exit
  rule 2
    action permit
    match protocol tcp
    match destination-port 8443
    enable
  exit
  rule 3
    action permit
    match protocol tcp
    match destination-port 80
    enable
  exit
  rule 4
    action permit
    match protocol tcp
    match destination-port 8080
    enable
  exit
exit

ip access-list extended INTERNET
   rule 1
    action permit
    enable
  exit
exit
```

```
ip access-list extended unauthUSER
  rule 1
    action permit
    match protocol udp
    match source-port 68
    match destination-port 67
    enable
  exit
  rule 2
    action permit
    match protocol udp
    match destination-port 53
    enable
  exit
exit

subscriber-control filters-server-url http://192.168.42.178:7070/filters/file
subscriber-control
  aaa das-profile COA
  aaa sessions-radius-profile PCRF
  aaa services-radius-profile PCRF
  nas-interface bridge 1
  session mac-authentication
  bypass-traffic-acl unauthUSER
  default-service
    class-map unauthUSER
    filter-name remote gosuslugi
    filter-action permit
    default-action redirect http://192.168.42.178:8080/eltex_portal/
    session-timeout 600
  exit
  enable
exit
snmp-server
snmp-server system-shutdown
snmp-server community "public11" ro
snmp-server community "private1" rw

snmp-server host 192.168.42.178
  source-interface bridge 1
exit
```

snmp-server enable traps
snmp-server enable traps config
snmp-server enable traps config commit
snmp-server enable traps config confirm
snmp-server enable traps environment
snmp-server enable traps environment memory-flash-critical-low
snmp-server enable traps environment memory-flash-low
snmp-server enable traps environment memory-ram-critical-low
snmp-server enable traps environment memory-ram-low
snmp-server enable traps environment cpu-load
snmp-server enable traps environment cpu-critical-temp
snmp-server enable traps environment cpu-overheat-temp
snmp-server enable traps environment cpu-supercooling-temp
snmp-server enable traps file-operations
snmp-server enable traps file-operations successful
snmp-server enable traps file-operations failed
snmp-server enable traps file-operations canceled
snmp-server enable traps interfaces
snmp-server enable traps interfaces rx-utilization-high
snmp-server enable traps interfaces tx-utilization-high
snmp-server enable traps interfaces number-high
snmp-server enable traps bras
snmp-server enable traps bras sessions-number-high
snmp-server enable traps screen
snmp-server enable traps screen dest-limit
snmp-server enable traps screen source-limit
snmp-server enable traps screen icmp-threshold
snmp-server enable traps screen udp-threshold
snmp-server enable traps screen syn-flood
snmp-server enable traps screen land
snmp-server enable traps screen winnuke
snmp-server enable traps screen icmp-frag
snmp-server enable traps screen udp-frag
snmp-server enable traps screen icmp-large
snmp-server enable traps screen syn-frag
snmp-server enable traps screen unknown-proto
snmp-server enable traps screen ip-frag
snmp-server enable traps screen port-scan
snmp-server enable traps screen ip-sweep
snmp-server enable traps screen syn-fin
snmp-server enable traps screen fin-no-ack
snmp-server enable traps screen no-flag
snmp-server enable traps screen spoofing
snmp-server enable traps screen reserved
snmp-server enable traps screen quench
snmp-server enable traps screen echo-request
snmp-server enable traps screen time-exceeded
snmp-server enable traps screen unreachable
snmp-server enable traps screen tcp-all-flags
snmp-server enable traps entity
snmp-server enable traps entity config-change
snmp-server enable traps entity-sensor
snmp-server enable traps entity-sensor threshold
snmp-server enable traps envmon
snmp-server enable traps envmon shutdown
snmp-server enable traps envmon temperature
snmp-server enable traps flash
snmp-server enable traps flash insertion
snmp-server enable traps flash removal
snmp-server enable traps snmp
snmp-server enable traps snmp authentication
snmp-server enable traps snmp coldstart
snmp-server enable traps snmp linkdown
snmp-server enable traps snmp linkup
snmp-server enable traps syslog

```
bridge 1
  security-zone trusted
  ip address dhcp
  ip dhcp client ignore dns-nameserver
  ip dhcp client ignore router
  enable
exit
bridge 11
  security-zone user
  ip address 192.168.1.1/24
  service-subscriber-control any
  location SSID12
  enable
exit

interface gigabitethernet 1/0/1
  description "UPLink"
  ip address dhcp
  security-zone untrusted
exit
interface gigabitethernet 1/0/1.701
   bridge-group 11
exit
interface gigabitethernet 1/0/1.702
  bridge-group 11
exit
interface gigabitethernet 1/0/2
   shutdown
exit
interface gigabitethernet 1/0/3
  shutdown
exit
interface gigabitethernet 1/0/4
  shutdown
exit
interface gigabitethernet 1/0/5
  shutdown
exit
interface gigabitethernet 1/0/6
  shutdown
exit
interface loopback 1
exit
tunnel gre 1
  keepalive retries 3
  keepalive dhcp dependent-interface bridge 1
  keepalive dhcp dependent-interface gi1/0/1
  mode ethernet
  local address xauth ipsec_vpn
  remote address xauth ipsec_vpn management-ip
enable
exit
tunnel gre 1.1
   bridge-group 1
  snmp init-trap
  enable
exit
```

```
security zone-pair untrusted self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair trusted self
  rule 1
    action permit
    enable
  exit
exit
security zone-pair user untrusted
  rule 10
    action permit
    enable
  exit
exit
security zone-pair user self
  rule 10
    action permit
    match protocol udp
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
  exit
  rule 20
    action permit
    match protocol tcp
    match destination-port redirect
    enable
  exit
  rule 30
    action permit
    match protocol udp
    match destination-port dns
    enable
  exit
exit

access profile acc_p
exit

security ike proposal ike_prop
exit

security ike policy ike_pol
  authentication method xauth-psk-key
  authentication mode client
  proposal ike_prop
exit

security ike gateway ike_gw
  ike-policy ike_pol
  assign-interface loopback 1
  local interface gigabitethernet 1/0/1
  remote network dynamic client
  mode policy-based
  dead-peer-detection action restart
  dead-peer-detection interval 10
exit

security ipsec proposal ipsec_prop
exit

security ipsec policy ipsec_pol
  proposal ipsec_prop
exit

security ipsec vpn ipsec_vpn
  mode ike
  ike establish-tunnel immediate
  ike gateway ike_gw
  ike ipsec-policy ipsec_pol
  enable
exit
```

```
nat source
 ruleset NAT
  to interface gigabitethernet 1/0/1
  rule 10
   match source-address natpool
   action source-nat interface
   enable
  exit
  exit
exit

ip dhcp-server
ip dhcp-server pool lan
 network 192.168.1.0/24
 max-lease-time 000:00:20
 default-lease-time 000:00:10
 address-range 192.168.1.2-192.168.1.254
 default-router 192.168.1.1
 dns-server 192.168.1.1
exit

ip ssh server

clock timezone gmt +7

ntp enable
ntp server 100.123.0.2
exit
```

"".

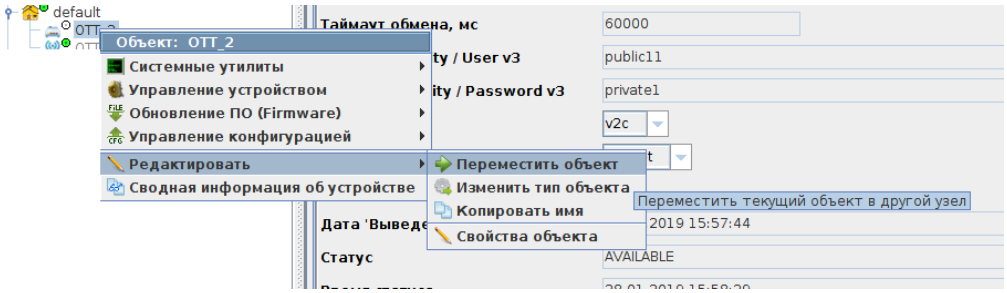
ESR-10 OTT

, OTT ESR . :

1) OTT ESR-10

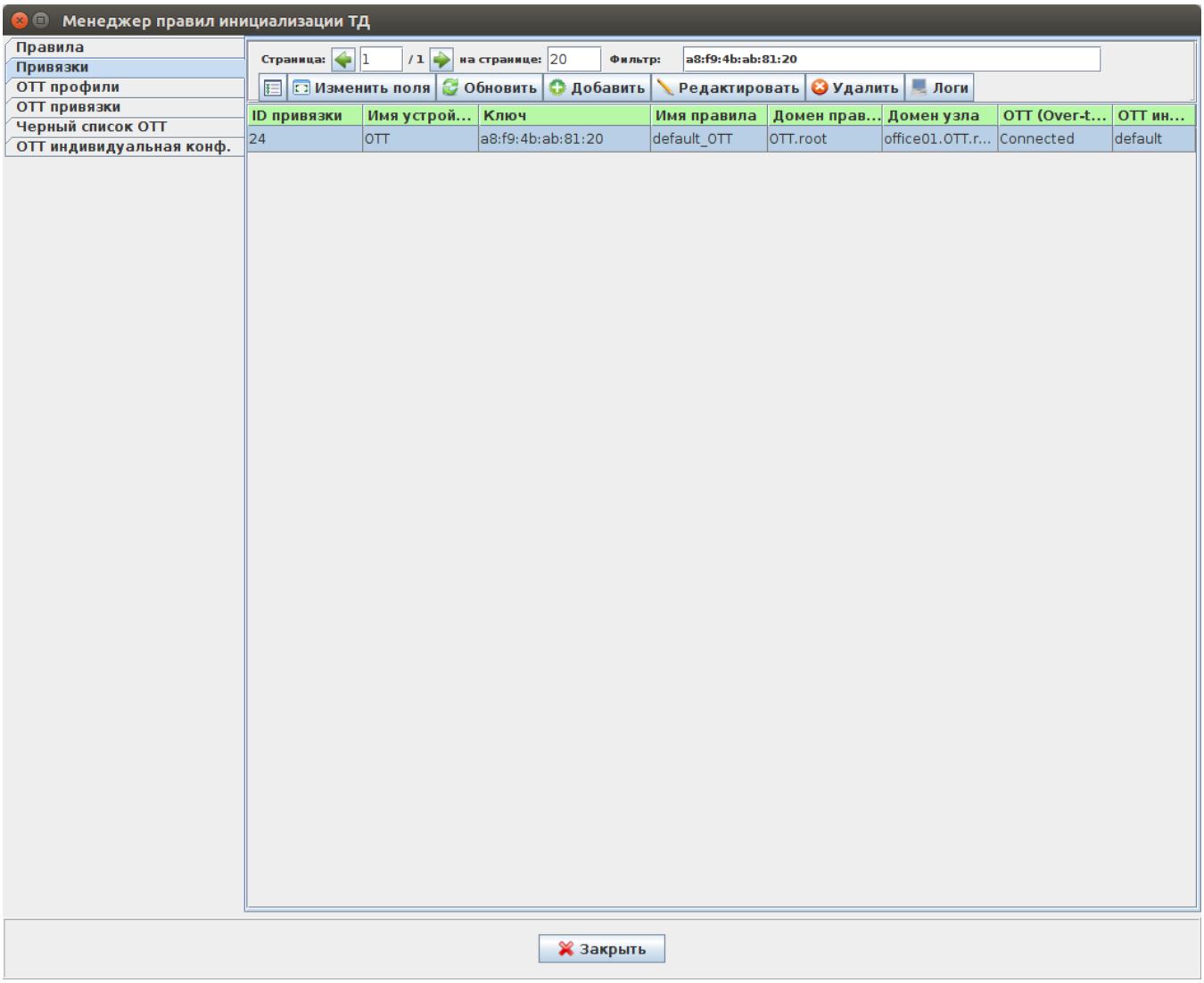
MAC- ESR-10 .

1. OTT, :

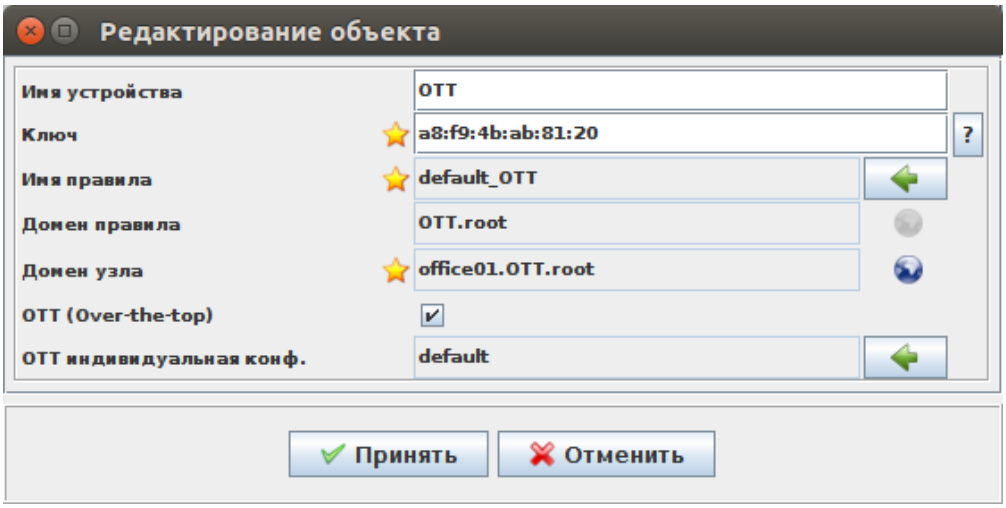


OTT.

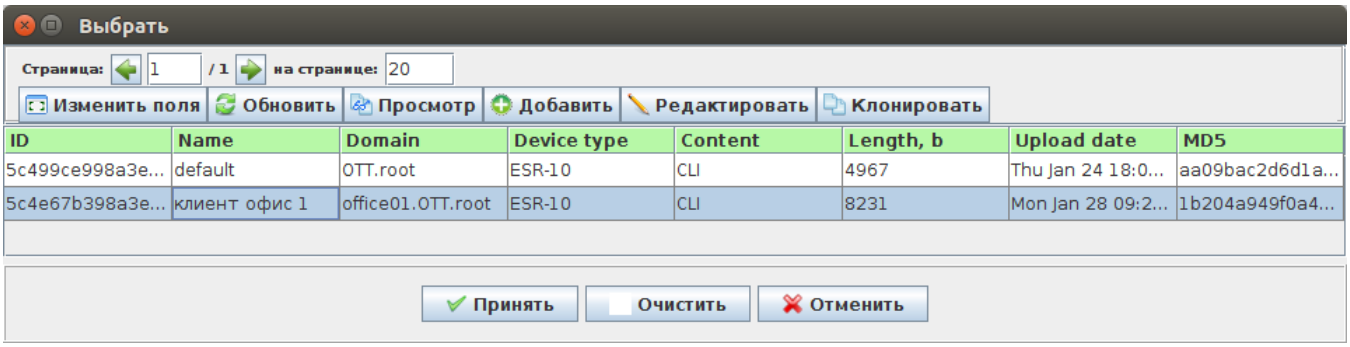
2. "Wireless" " " "" :


Менеджер правил инициализации ТД
Правила
Привязки
OTT профили
OTT привязки
Черный список OTT
OTT индивидуальная конф.
Страница: 1 / 1 на странице: 20 Фильтр: a8:f9:4b:ab:81:20
Изменить поля
Обновить
Добавить
Редактировать
Удалить
Логи
ID привязки
Имя устрой...
Ключ
Имя правила
Домен прав...
Домен узла
OTT (Over-t...
OTT ин...
24
OTT
a8:f9:4b:ab:81:20
default_OTT
OTT.root
office01.OTT.r...
Connected
default
Закрыть

3. "" :

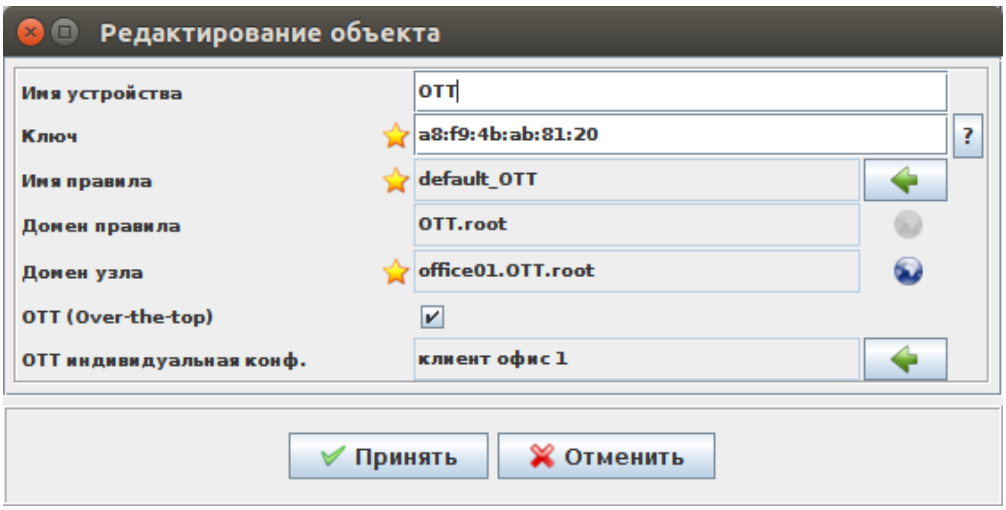

Редактирование объекта
Имя устройства
OTT
Ключ
a8:f9:4b:ab:81:20
?
Имя правила
default_OTT
Домен правила
OTT.root
Домен узла
office01.OTT.root
OTT (Over-the-top)
OTT индивидуальная конф.
default
Принять
Отменить

4. "OTT ." ESR-10 :



"".

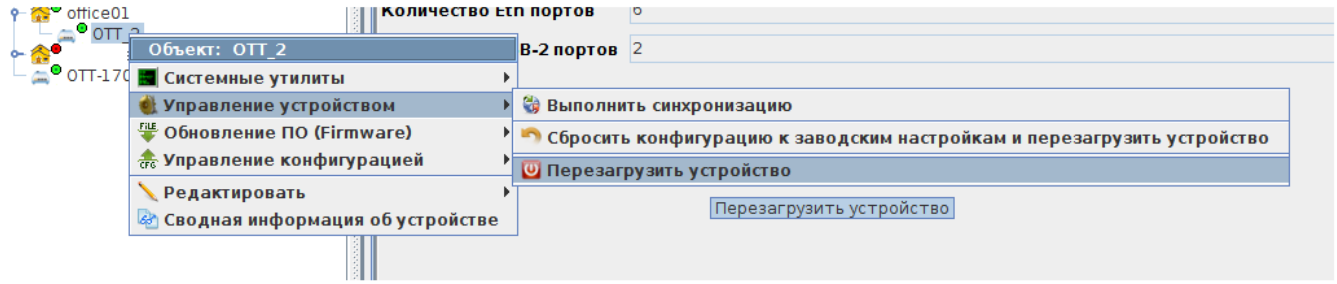
5. , "OTT ." :



"".

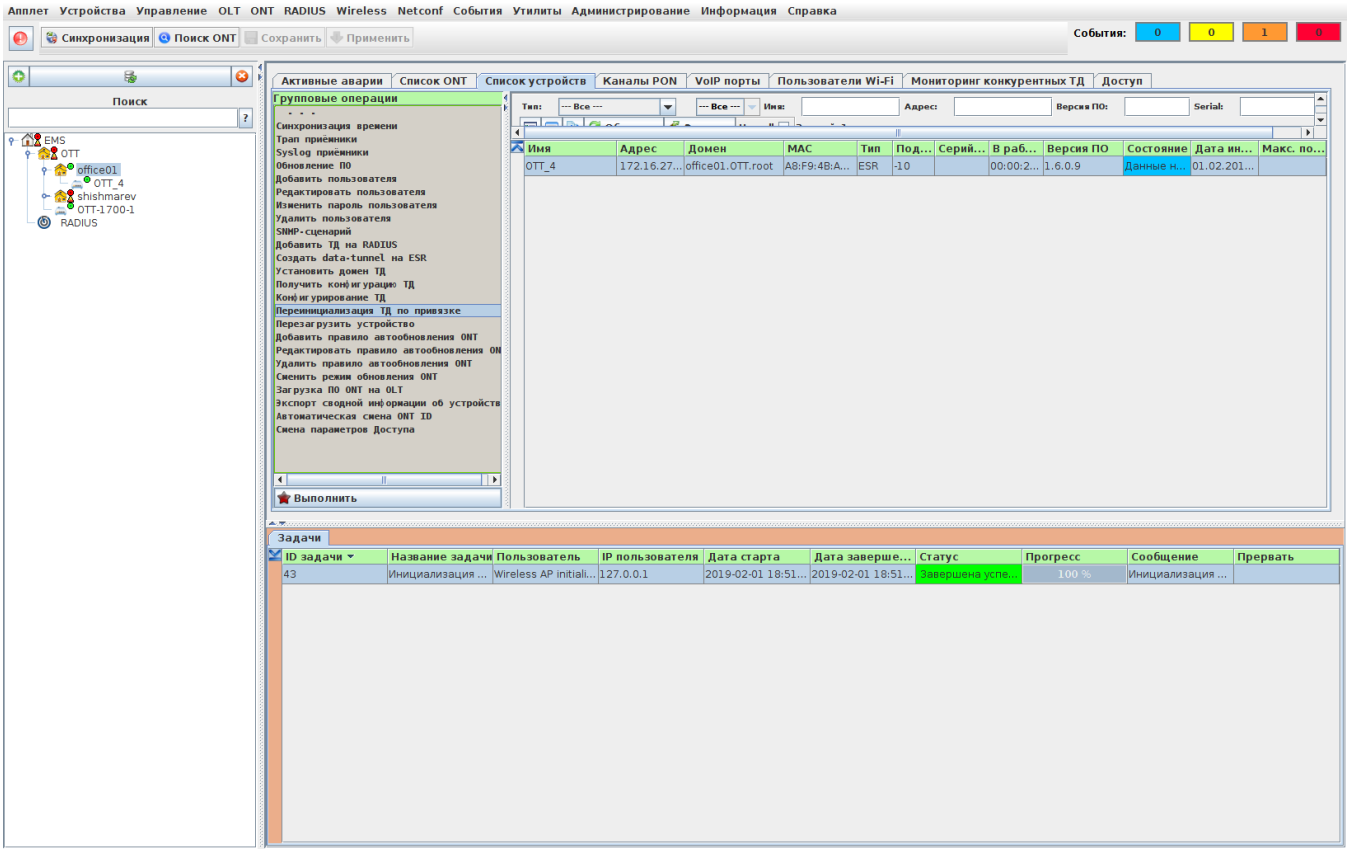
" ".

5. ESR-10 " " " ".

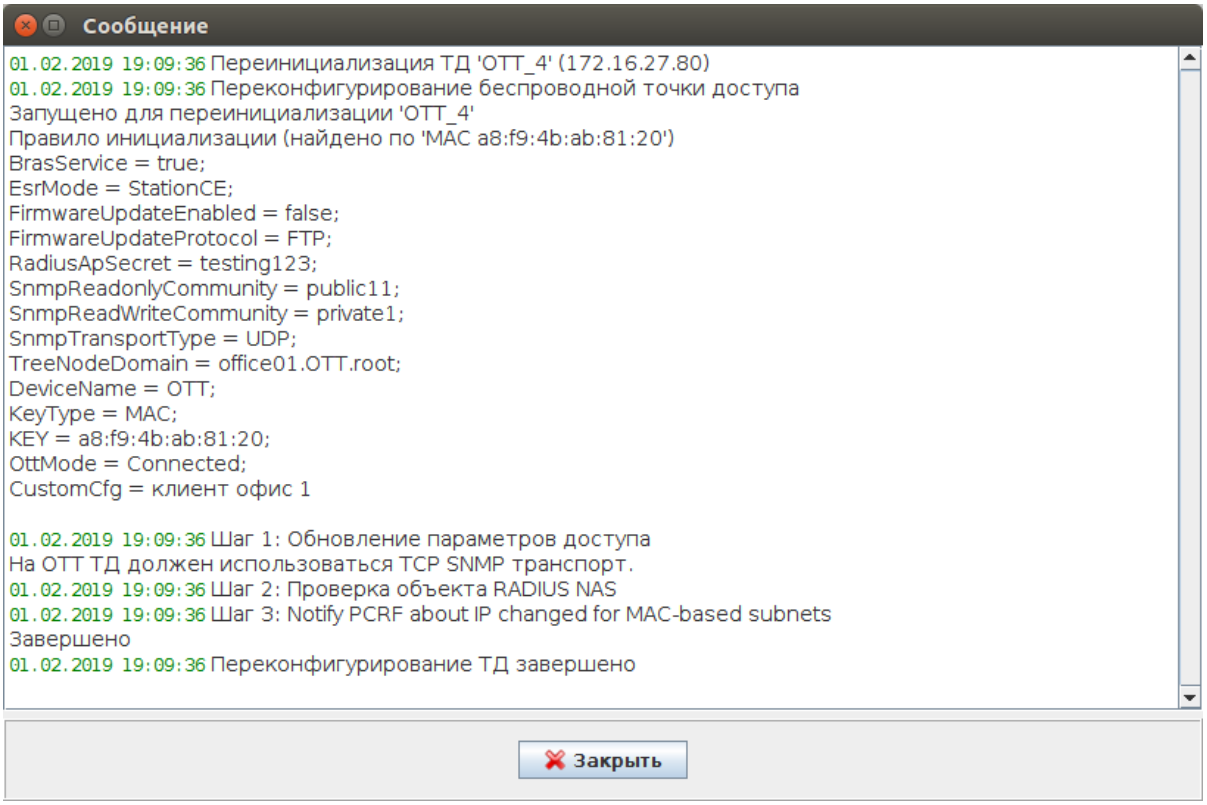


, SA .

6. . , , " " " " " ", ESR-10 "":


Апплет Устройства Управление OLT ONT RADIUS Wireless Netconf События Утилиты Администрирование Информация Справка
Синхронизация
Поиск ONT
Сохранить
Применить
События:
Поиск
EMS
OTT
office01
OTT_4
shishmarev
OTT-1700-1
RADIUS
Активные аварии
Список ONT
Список устройств
Каналы PON
VoIP порты
Пользователи Wi-Fi
Мониторинг конкурентных ТД
Доступ
Групповые операции
Синхронизация времени
Трап приёмники
Syslog приёмники
Обновление ПО
Добавить пользователя
Редактировать пользователя
Изменить пароль пользователя
Удалить пользователя
SNMP-сценарий
Добавить ТД на RADIUS
Создать data-tunnel на ESR
Установить домен ТД
Получить конфигурацию ТД
Конфигурирование ТД
Переинициализация ТД по привязке
Перезагрузить устройство
Добавить правило автообновления ONT
Редактировать правило автообновления ON
Удалить правило автообновления ONT
Сменить режим обновления ONT
Загрузка ПО ONT на OLT
Экспорт сводной информации об устройств
Автоматическая смена ONT ID
Смена параметров Доступа
Выполнить
Имя
Адрес
Домен
MAC
Тип
Под...
Серий...
В раб...
Версия ПО
Состояние
Дата ин...
Макс. по...
OTT_4
172.16.27...
office01.OTT.root
A8:F9:4B:A...
ESR
-10
00:00:2...
1.6.0.9
Данные н...
01.02.201...
Задачи
ID задачи
Название задачи
Пользователь
IP пользователя
Дата старта
Дата заверше...
Статус
Прогресс
Сообщение
Прервать
43
Инициализация ...
Wireless AP initiali...
127.0.0.1
2019-02-01 18:51...
2019-02-01 18:51...
Завершена успе...
100 %
Инициализация ...

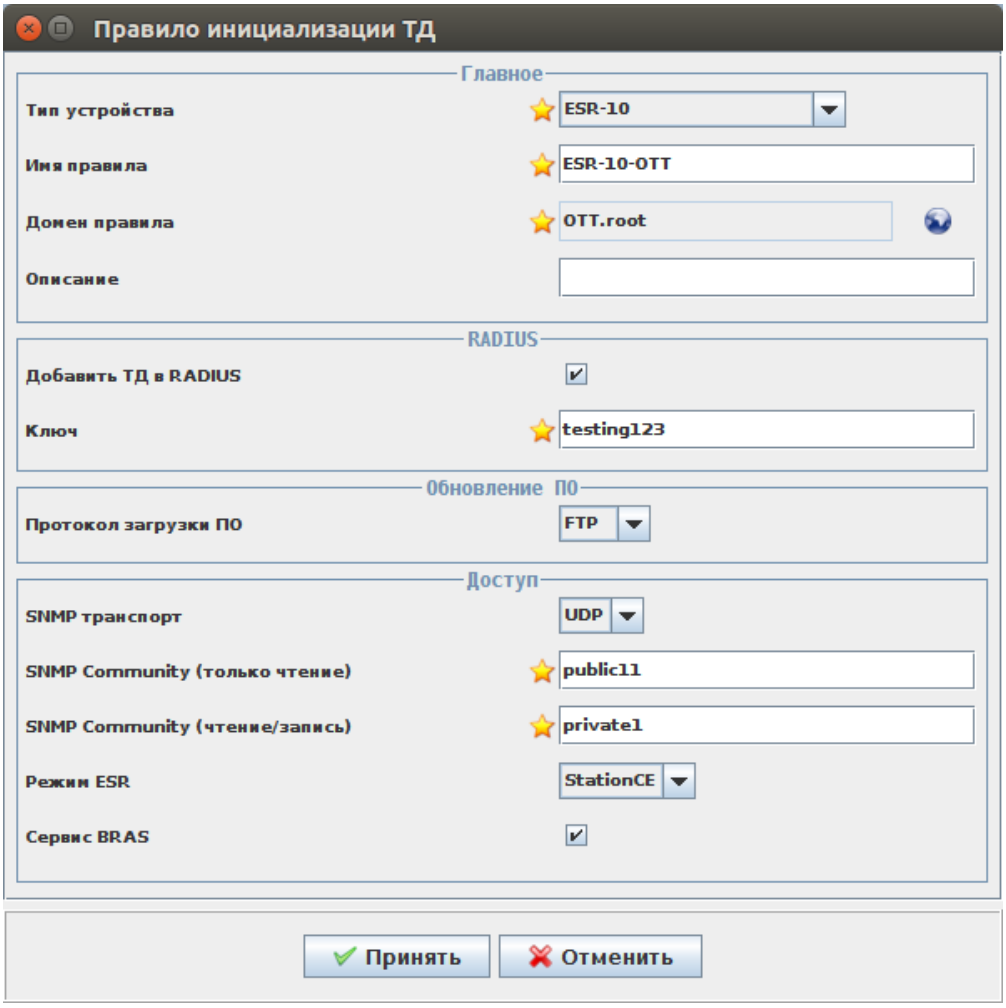
"" :


Сообщение
01.02.2019 19:09:36 Переинициализация ТД 'OTT_4' (172.16.27.80)
01.02.2019 19:09:36 Переконфигурирование беспроводной точки доступа
Запущено для переинициализации 'OTT_4'
Правило инициализации (найдено по 'MAC a8:f9:4b:ab:81:20')
BrasService = true;
EsrMode = StationCE;
FirmwareUpdateEnabled = false;
FirmwareUpdateProtocol = FTP;
RadiusApSecret = testing123;
SnmpReadonlyCommunity = public11;
SnmpReadWriteCommunity = private1;
SnmpTransportType = UDP;
TreeNodeDomain = office01.OTT.root;
DeviceName = OTT;
KeyType = MAC;
KEY = a8:f9:4b:ab:81:20;
OttMode = Connected;
CustomCfg = клиент офис 1
01.02.2019 19:09:36 Шаг 1: Обновление параметров доступа
На OTT ТД должен использоваться TCP SNMP транспорт.
01.02.2019 19:09:36 Шаг 2: Проверка объекта RADIUS NAS
01.02.2019 19:09:36 Шаг 3: Notify PCRF about IP changed for MAC-based subnets
Завершено
01.02.2019 19:09:36 Переконфигурирование ТД завершено
Закрыть

7. - .

2) EMS OTT, , MAC- ,

1. ESR-10 OTT. "Wireless" " " "" "":



:

1) " " - "ESR-10";

2) " " - "ESR-10-OTT" ( );

3) " RADIUS" - ;

4) "" - "testing123";

5) " " - "FTP";

6) "SNMP " - "UDP";

7) "SNMP Community ( )" - "public11" (ESR - 8);

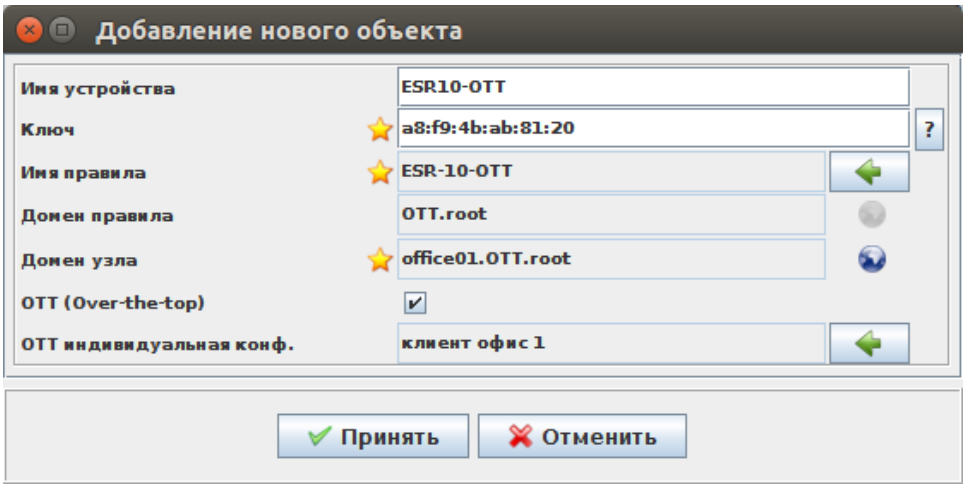
8) "SNMP Community (/)" - "private1";

9) ESR - "StationCE" (, , PCRF /);

10) " BRAS" - (ESR10 OTT , , OTT).

"".

2. "Wireless" " " "" "":



:

1) " " - , EMS;

2) "" - MAC- ESR-10;

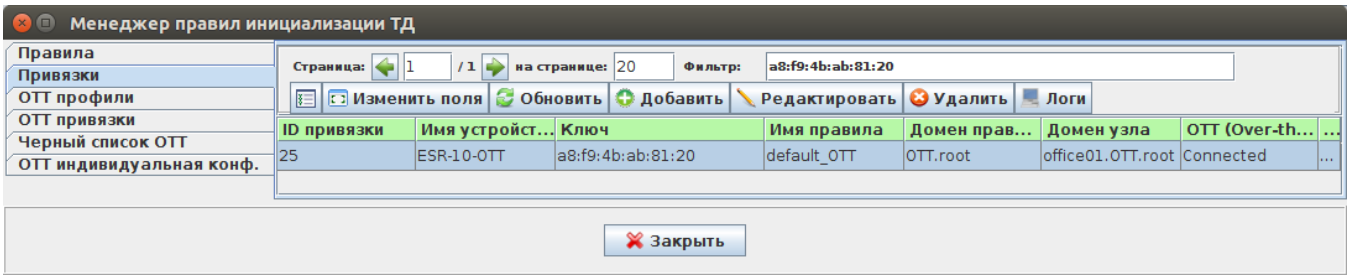
3) " " - ;

4) " " - , ;

5) OTT (Over-the-top) - ;

6) OTT . - , .

"":



, .

ESR-10 .

OTT , -

, ESR-10 - (SA) - IPsec, update-timer wait-timer, (admin) JSON, c - CLi CLi . .

ESR-10 SA: OTT , -

CLI SA - , , SA , wait-timer ESR-10 SA .

- , SA , wait-timer ESR-10 SA .

, - , .

, - IPsec - . .

, ESR-10 CLi SA "OTT ." . , uplink, IPsec, GRE , .. (wait-timer ESR-10 factory-config SA).

OTT 43 15 (bridge 1) . wait-timer, - . factory-config, - . wait-timer -.

SSID .

- . , - - L2 (location, ; location , gi1/0/2 gi1/0/2.100).

default OTT

default, IPsec, . . ESR-10 , EMS, . , , MAC ESR10 . ESR-10 , , . .

, ESR-10, SA. , "OTT ." .

```
hostname ESR10-OTT

object-group network SoftWLC
 ip address-range 192.168.42.178
exit

line console # ESR10
 aaa disable
exit

security zone trusted
exit
security zone untrusted
exit

snmp-server
snmp-server system-shutdown
snmp-server community "public11" ro
snmp-server community "private1" rw

snmp-server host 192.168.42.178
source-interface bridge 1
exit

snmp-server enable traps
snmp-server enable traps config
snmp-server enable traps config commit
snmp-server enable traps config confirm
snmp-server enable traps environment
snmp-server enable traps environment memory-flash-critical-low
snmp-server enable traps environment memory-flash-low
snmp-server enable traps environment memory-ram-critical-low
snmp-server enable traps environment memory-ram-low
snmp-server enable traps environment cpu-load
snmp-server enable traps environment cpu-critical-temp
snmp-server enable traps environment cpu-overheat-temp
snmp-server enable traps environment cpu-supercooling-temp
snmp-server enable traps file-operations
snmp-server enable traps file-operations successful
snmp-server enable traps file-operations failed
snmp-server enable traps file-operations canceled
snmp-server enable traps interfaces
snmp-server enable traps interfaces rx-utilization-high
snmp-server enable traps interfaces tx-utilization-high
snmp-server enable traps interfaces number-high
snmp-server enable traps screen
snmp-server enable traps screen dest-limit
snmp-server enable traps screen source-limit
snmp-server enable traps screen icmp-threshold
snmp-server enable traps screen udp-threshold
snmp-server enable traps screen syn-flood
snmp-server enable traps screen land
snmp-server enable traps screen winnuke
snmp-server enable traps screen icmp-frag
snmp-server enable traps screen udp-frag
snmp-server enable traps screen icmp-large
snmp-server enable traps screen syn-frag
```

```
snmp-server enable traps screen unknown-proto
snmp-server enable traps screen ip-frag
snmp-server enable traps screen port-scan
snmp-server enable traps screen ip-sweep
snmp-server enable traps screen syn-fin
snmp-server enable traps screen fin-no-ack
snmp-server enable traps screen no-flag
snmp-server enable traps screen spoofing
snmp-server enable traps screen reserved
snmp-server enable traps screen quench
snmp-server enable traps screen echo-request
snmp-server enable traps screen time-exceeded
snmp-server enable traps screen unreachable
snmp-server enable traps screen tcp-all-flags
snmp-server enable traps entity
snmp-server enable traps entity config-change
snmp-server enable traps entity-sensor
snmp-server enable traps entity-sensor threshold
snmp-server enable traps envmon
snmp-server enable traps envmon shutdown
snmp-server enable traps envmon temperature
snmp-server enable traps flash
snmp-server enable traps flash insertion
snmp-server enable traps flash removal
snmp-server enable traps snmp
snmp-server enable traps snmp authentication
snmp-server enable traps snmp coldstart
snmp-server enable traps snmp linkdown
snmp-server enable traps snmp linkup
snmp-server enable traps syslog

bridge 1 #bridge 1     ,
  security-zone trusted
  ip address dhcp
  ip dhcp client ignore router
  enable
exit

interface gigabitethernet 1/0/1 # gi1/0/1     ,
  description "UPLink"
  ip address dhcp
  security-zone untrusted
exit
interface gigabitethernet 1/0/2
  shutdown
exit
interface gigabitethernet 1/0/3
  shutdown
exit
interface gigabitethernet 1/0/4
  shutdown
exit
interface gigabitethernet 1/0/5
  shutdown
exit
interface gigabitethernet 1/0/6
  shutdown
exit
interface loopback 1
exit
tunnel gre 1 # GRE   -
  mtu 1356 #  -   SA (ipsec gre-mtu-offset)
  keepalive retries 3 #  -   SA (ipsec gre-ping-counter)
  keepalive dst-address 10.2.0.1 #  -   DHCP  43  15
  keepalive dhcp dependent-interface bridge 1
  keepalive dhcp dependent-interface gi1/0/1
  keepalive enable #  - GRE keepalive   .    DHCP  43  15
  mode ethernet
  local address xauth ipsec_vpn #    mode-cfg   IPsec ,  IPsec VPN
  remote address xauth ipsec_vpn management-ip #    mode-cfg   IPsec ,  IPsec VPN
  enable
exit
tunnel gre 1.1 # sub-GRE   -
  bridge-group 1
  mtu 1352 #  -   SA (ipsec gre-mtu-offset)
  snmp init-trap
  enable
exit
```

```
security zone-pair untrusted self
 rule 1
  action permit
  match protocol icmp
  enable
 exit
exit
security zone-pair trusted self
 rule 1
  action permit
  match source-address SoftWLC
  enable
 exit
exit

access profile acc_p # ,
 user a8:f9:4b:ab:81:20 #  -   SA (ipsec xauth-user)
  password ascii-text encrypted 9FB30B49E43D47FAC32E0994C89C75B81313F0F038CC02FC #   -   SA (ipsec xauth-password)
 exit
exit

security ike proposal ike_prop # ,
 authentication algorithm md5 #  -   SA (ipsec auth-alg)
 encryption algorithm aes128 #  -   SA (ipsec encrypt-alg)
 dh-group 1 #  -   SA (ipsec dh-group)
exit

security ike policy ike_pol # ,
 lifetime seconds 86400 #  -   SA (ipsec lifetime)
 pre-shared-key ascii-text testing123 #  -   SA (ipsec password)
 authentication method xauth-psk-key
 authentication mode client
 proposal ike_prop
exit

security ike gateway ike_gw # ,
 ike-policy ike_pol
 assign-interface loopback 1
 local interface gigabitethernet 1/0/1
 remote address 100.64.0.1 #  -   SA (ipsec remote-gateway)
 remote network dynamic client
 mode policy-based
 dead-peer-detection action restart
 dead-peer-detection interval 10
 dead-peer-detection timeout 60 #  -   SA (ipsec dpd-delay)
 xauth access-profile acc_p client a8:f9:4b:ab:81:20 #  -       SA xauth-user
exit

security ipsec proposal ipsec_prop # ,
 authentication algorithm md5 #  -   SA (ipsec sa-auth-alg)
 encryption algorithm aes128 #  -   SA (ipsec sa-encrypt-alg)
exit

security ipsec policy ipsec_pol # ,
 lifetime seconds 3600 #  -   SA (ipsec sa-lifetime)
 proposal ipsec_prop
exit



security ipsec vpn ipsec_vpn # ,
 mode ike
 ike establish-tunnel immediate
 ike gateway ike_gw
 ike ipsec-policy ipsec_pol
 enable
exit

ip ssh server
```

, custom-config

```
hostname ESR10-OTT

object-group network SoftWLC
  ip address-range 100.123.0.2
exit

syslog console debug
syslog monitor info

line console

  aaa disable

exit


security zone trusted
exit
security zone untrusted
exit

snmp-server
snmp-server system-shutdown
snmp-server community "public11" ro
snmp-server community "private1" rw

snmp-server host 100.123.0.2

source-interface bridge 1
exit



snmp-server enable traps
snmp-server enable traps config
snmp-server enable traps config commit
snmp-server enable traps config confirm
snmp-server enable traps environment
snmp-server enable traps environment memory-flash-critical-low
snmp-server enable traps environment memory-flash-low
snmp-server enable traps environment memory-ram-critical-low
snmp-server enable traps environment memory-ram-low
snmp-server enable traps environment cpu-load
snmp-server enable traps environment cpu-critical-temp
snmp-server enable traps environment cpu-overheat-temp
snmp-server enable traps environment cpu-supercooling-temp
snmp-server enable traps file-operations
snmp-server enable traps file-operations successful
snmp-server enable traps file-operations failed
snmp-server enable traps file-operations canceled
snmp-server enable traps interfaces
snmp-server enable traps interfaces rx-utilization-high
snmp-server enable traps interfaces tx-utilization-high
snmp-server enable traps interfaces number-high
snmp-server enable traps bras
snmp-server enable traps bras sessions-number-high
snmp-server enable traps screen
snmp-server enable traps screen dest-limit
snmp-server enable traps screen source-limit
snmp-server enable traps screen icmp-threshold
snmp-server enable traps screen udp-threshold
snmp-server enable traps screen syn-flood
snmp-server enable traps screen land
snmp-server enable traps screen winnuke
snmp-server enable traps screen icmp-frag
snmp-server enable traps screen udp-frag
snmp-server enable traps screen icmp-large
snmp-server enable traps screen syn-frag
snmp-server enable traps screen unknown-proto
snmp-server enable traps screen ip-frag
snmp-server enable traps screen port-scan
snmp-server enable traps screen ip-sweep
snmp-server enable traps screen syn-fin
snmp-server enable traps screen fin-no-ack
snmp-server enable traps screen no-flag
snmp-server enable traps screen spoofing
snmp-server enable traps screen reserved
snmp-server enable traps screen quench
snmp-server enable traps screen echo-request
snmp-server enable traps screen time-exceeded
```

```
snmp-server enable traps screen unreachable
snmp-server enable traps screen tcp-all-flags
snmp-server enable traps entity
snmp-server enable traps entity config-change
snmp-server enable traps entity-sensor
snmp-server enable traps entity-sensor threshold
snmp-server enable traps envmon
snmp-server enable traps envmon shutdown
snmp-server enable traps envmon temperature
snmp-server enable traps flash
snmp-server enable traps flash insertion
snmp-server enable traps flash removal
snmp-server enable traps snmp
snmp-server enable traps snmp authentication
snmp-server enable traps snmp coldstart
snmp-server enable traps snmp linkdown
snmp-server enable traps snmp linkup
snmp-server enable traps syslog

bridge 1
  security-zone trusted
  ip address dhcp
  ip dhcp client ignore router
  enable
exit

interface gigabitethernet 1/0/1
  description "UPLink"
  ip address dhcp
  security-zone untrusted
  service-policy dynamic all
exit
interface gigabitethernet 1/0/2
  shutdown
exit
interface gigabitethernet 1/0/3
  shutdown
exit
interface gigabitethernet 1/0/4
  shutdown
exit
interface gigabitethernet 1/0/5
  shutdown
exit
interface gigabitethernet 1/0/6
  shutdown
exit
interface loopback 1
exit
tunnel gre 1
  keepalive dhcp dependent-interface bridge 1
  keepalive dhcp dependent-interface gi1/0/1
  mode ethernet
  local address xauth ipsec_vpn
  remote address xauth ipsec_vpn management-ip
  enable
exit
tunnel gre 1.1
  bridge-group 1
  snmp init-trap
  enable
exit

security zone-pair untrusted self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair trusted self
  rule 1
    action permit
    match source-address SoftWLC
    enable
  exit
exit

access profile acc_p
```

```
exit

security ike proposal ike_prop
exit

security ike policy ike_pol
  authentication method xauth-psk-key
  authentication mode client
  proposal ike_prop
exit

security ike gateway ike_gw
  ike-policy ike_pol
  assign-interface loopback 1
  local interface gigabitethernet 1/0/1
  remote network dynamic client
  mode policy-based
  dead-peer-detection action restart
  dead-peer-detection interval 10
exit

security ipsec proposal ipsec_prop
exit

security ipsec policy ipsec_pol
   proposal ipsec_prop
exit



security ipsec vpn ipsec_vpn
  mode ike
  ike establish-tunnel immediate
  ike gateway ike_gw
  ike ipsec-policy ipsec_pol
  enable
exit

ip ssh server
```

, OTT . () , . SSID -, - , .. . SSID gi1/0/2-6 (gi1/0/1) mode access , . NAT .

, gi1/0/1, SSID1 2314, SSID2 2315. - bridge 11. NAT gi1/0/1.

```
hostname ESR10-OTT-BR-1

ip firewall sessions classification enable
object-group service dns
   port-range 53
exit
object-group service dhcp_server
  port-range 67
exit
object-group service dhcp_client
  port-range 68
exit
object-group service redirect
port-range 3128-3129
port-range 3130-3131
exit

object-group network natpool
   ip prefix 198.19.253.0/24
exit
object-group network SoftWLC
  ip address-range 192.168.42.178
exit
```

```
radius-server timeout 10
radius-server retransmit 5
radius-server host 192.168.42.178
  key ascii-text encrypted 88B11079B9014FAAF7B9
  timeout 11
  priority 20
  source-interface bridge 1
  auth-port 31812
  acct-port 31813
  retransmit 10
  dead-interval 10
exit
aaa radius-profile PCRF
  radius-server host 192.168.42.178
exit
das-server COA
  key ascii-text encrypted 88B11079B9014FAAF7B9
  port 3799
  clients object-group SoftWLC
exit
aaa das-profile COA
  das-server COA
exit

line console
  aaa disable
exit

domain lookup enable

security zone trusted
exit
security zone untrusted
exit
security zone user
exit

ip access-list extended WELCOME
  rule 1
    action permit
    match protocol tcp
    match destination-port 443
    enable
  exit
  rule 2
    action permit
    match protocol tcp
    match destination-port 8443
    enable
  exit
  rule 3
    action permit
    match protocol tcp
    match destination-port 80
    enable
  exit
  rule 4
    action permit
    match protocol tcp
    match destination-port 8080
    enable
 exit
exit

ip access-list extended INTERNET
  rule 1
    action permit
    enable
  exit
exit
```

```
ip access-list extended unauthUSER
  rule 1
    action permit
    match protocol udp
    match source-port 68
    match destination-port 67
    enable
  exit
  rule 2
    action permit
    match protocol udp
    match destination-port 53
    enable
  exit
exit

subscriber-control filters-server-url http://192.168.42.178:7070/filters/file
subscriber-control
  aaa das-profile COA
  aaa sessions-radius-profile PCRF
  aaa services-radius-profile PCRF
  nas-interface bridge 1
  session mac-authentication
  bypass-traffic-acl unauthUSER
  default-service
    class-map unauthUSER
    filter-name remote gosuslugi
    filter-action permit
    default-action redirect http://192.168.42.178:8080/eltex_portal/
    session-timeout 600
  exit
  enable
exit
snmp-server
snmp-server system-shutdown
snmp-server community "public11" ro
snmp-server community "private1" rw

snmp-server host 192.168.42.178
  source-interface bridge 1
exit
```

```
snmp-server enable traps
snmp-server enable traps config
snmp-server enable traps config commit
snmp-server enable traps config confirm
snmp-server enable traps environment
snmp-server enable traps environment memory-flash-critical-low
snmp-server enable traps environment memory-flash-low
snmp-server enable traps environment memory-ram-critical-low
snmp-server enable traps environment memory-ram-low
snmp-server enable traps environment cpu-load
snmp-server enable traps environment cpu-critical-temp
snmp-server enable traps environment cpu-overheat-temp
snmp-server enable traps environment cpu-supercooling-temp
snmp-server enable traps file-operations
snmp-server enable traps file-operations successful
snmp-server enable traps file-operations failed
snmp-server enable traps file-operations canceled
snmp-server enable traps interfaces
snmp-server enable traps interfaces rx-utilization-high
snmp-server enable traps interfaces tx-utilization-high
snmp-server enable traps interfaces number-high
snmp-server enable traps bras
snmp-server enable traps bras sessions-number-high
snmp-server enable traps screen
snmp-server enable traps screen dest-limit
snmp-server enable traps screen source-limit
snmp-server enable traps screen icmp-threshold
snmp-server enable traps screen udp-threshold
snmp-server enable traps screen syn-flood
snmp-server enable traps screen land
snmp-server enable traps screen winnuke
snmp-server enable traps screen icmp-frag
snmp-server enable traps screen udp-frag
snmp-server enable traps screen icmp-large
snmp-server enable traps screen syn-frag
snmp-server enable traps screen unknown-proto
snmp-server enable traps screen ip-frag
snmp-server enable traps screen port-scan
snmp-server enable traps screen ip-sweep
snmp-server enable traps screen syn-fin
snmp-server enable traps screen fin-no-ack
snmp-server enable traps screen no-flag
snmp-server enable traps screen spoofing
snmp-server enable traps screen reserved
snmp-server enable traps screen quench
snmp-server enable traps screen echo-request
snmp-server enable traps screen time-exceeded
snmp-server enable traps screen unreachable
snmp-server enable traps screen tcp-all-flags
snmp-server enable traps entity
snmp-server enable traps entity config-change
snmp-server enable traps entity-sensor
snmp-server enable traps entity-sensor threshold
snmp-server enable traps envmon
snmp-server enable traps envmon shutdown
snmp-server enable traps envmon temperature
snmp-server enable traps flash
snmp-server enable traps flash insertion
snmp-server enable traps flash removal
snmp-server enable traps snmp
snmp-server enable traps snmp authentication
snmp-server enable traps snmp coldstart

bridge 1
  security-zone trusted
  ip address dhcp
  ip dhcp client ignore dns-nameserver
  ip dhcp client ignore router
  enable
exit
bridge 11
  security-zone user
  ip address 198.19.253.1/24
  service-subscriber-control any
  location SSID12
  enable
exit
```

```
interface gigabitethernet 1/0/1
  description "UPLink"
  ip address dhcp
  security-zone untrusted
  service-policy dynamic all
exit
interface gigabitethernet 1/0/1.2314
  bridge-group 11
exit
interface gigabitethernet 1/0/1.2315
  bridge-group 11
exit
interface gigabitethernet 1/0/2
  shutdown
exit
interface gigabitethernet 1/0/3
  shutdown
exit
interface gigabitethernet 1/0/4
  shutdown
exit
interface gigabitethernet 1/0/5
  shutdown
exit
interface gigabitethernet 1/0/6
  shutdown
exit
interface loopback 1
exit
tunnel gre 1
  keepalive retries 3
  keepalive dhcp dependent-interface bridge 1
  keepalive dhcp dependent-interface gi1/0/1
  mode ethernet
  local address xauth ipsec_vpn
  remote address xauth ipsec_vpn management-ip
  enable
exit
tunnel gre 1.1
  bridge-group 1
  snmp init-trap
  enable
exit
```

```
security zone-pair untrusted self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair trusted self
   rule 1
    action permit
   enable
  exit
exit
security zone-pair user untrusted
  rule 10
    action permit
    enable
  exit
exit
security zone-pair user self
  rule 10
    action permit
    match protocol udp
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
  exit
  rule 20
    action permit
    match protocol tcp
    match destination-port redirect
    enable
  exit
  rule 30
    action permit
    match protocol udp
    match destination-port dns
    enable
  exit
exit

access profile acc_p
exit

security ike proposal ike_prop
exit

security ike policy ike_pol
  authentication method xauth-psk-key
  authentication mode client
  proposal ike_prop
exit

security ike gateway ike_gw
  ike-policy ike_pol
  assign-interface loopback 1
  local interface gigabitethernet 1/0/1
  remote network dynamic client
  mode policy-based
  dead-peer-detection action restart
  dead-peer-detection interval 10
exit

security ipsec proposal ipsec_prop
exit

security ipsec policy ipsec_pol
  proposal ipsec_prop
exit

security ipsec vpn ipsec_vpn
  mode ike
  ike establish-tunnel immediate
  ike gateway ike_gw
  ike ipsec-policy ipsec_pol
  enable
exit
```

```
nat source
 ruleset NAT
  to interface gigabitethernet 1/0/1
  rule 10
   match source-address natpool
   action source-nat interface

   enable
  exit
 exit
exit

ip dhcp-server
 ip dhcp-server pool lan
 network 198.19.253.0/24
 max-lease-time 000:00:20
 default-lease-time 000:00:10
 address-range 198.19.253.2-198.19.253.254
 default-router 198.19.253.1
 dns-server 198.19.253.1
exit

ip ssh server

clock timezone gmt +7

ntp enable
ntp server 192.168.42.178
exit
```

, gi1/0/1, gi1/0/2 - 701; gi1/0/3 - , 701.

```
hostname ESR10-OTT-BR

ip firewall sessions classification enable
root login enable
tech-support login enable
object-group service dns
 port-range 53
exit
object-group service dhcp_server
 port-range 67
exit
object-group service dhcp_client
 port-range 68
exit
object-group service redirect
 port-range 3128-3129
 port-range 3130-3131
exit

object-group network natpool
 ip prefix 198.19.253.0/24
exit
object-group network SoftWLC
 ip address-range 192.168.42.178
exit

vlan 701
exit

radius-server timeout 10
radius-server retransmit 5
radius-server host 192.168.42.178
 key ascii-text encrypted 88B11079B9014FAAF7B9
 timeout 11
 priority 20
 source-interface bridge 1
 auth-port 31812
 acct-port 31813
 retransmit 10
 dead-interval 10
exit
aaa radius-profile PCRF
 radius-server host 192.168.42.178
exit
das-server COA
```

```
  key ascii-text encrypted 88B11079B9014FAAF7B9
  port 3799
  clients object-group SoftWLC
exit
aaa das-profile COA
  das-server COA
exit

line console
  aaa disable
exit

domain lookup enable

security zone trusted
exit
security zone untrusted
exit
security zone user
exit

ip access-list extended WELCOME
  rule 1
    action permit
    match protocol tcp
    match destination-port 443
    enable
  exit
  rule 2
    action permit
    match protocol tcp
    match destination-port 8443
    enable
  exit
  rule 3
    action permit
    match protocol tcp
    match destination-port 80
    enable
  exit
  rule 4
    action permit
    match protocol tcp
    match destination-port 8080
    enable
  exit
exit
ip access-list extended INTERNET
  rule 1
    action permit
    enable
  exit
exit

ip access-list extended unauthUSER
  rule 1
    action permit
    match protocol udp
    match source-port 68
    match destination-port 67
    enable
  exit
  rule 2
    action permit
    match protocol udp
    match destination-port 53
    enable
  exit
exit

subscriber-control filters-server-url http://192.168.42.178:7070/filters/file
subscriber-control
  aaa das-profile COA
  aaa sessions-radius-profile PCRF
  aaa services-radius-profile PCRF
  nas-interface bridge 1
  session mac-authentication
  bypass-traffic-acl unauthUSER
  default-service
```

```
    class-map unauthUSER
    filter-name remote gosuslugi
    filter-action permit
    default-action redirect http://192.168.42.178:8080/eltex_portal/
    session-timeout 600
   exit
   enable
exit
snmp-server
snmp-server system-shutdown
snmp-server community "public11" ro
snmp-server community "private1" rw

snmp-server host 192.168.42.178
  source-interface bridge 1
exit

snmp-server enable traps
snmp-server enable traps config
snmp-server enable traps config commit
snmp-server enable traps config confirm
snmp-server enable traps environment
snmp-server enable traps environment memory-flash-critical-low
snmp-server enable traps environment memory-flash-low
snmp-server enable traps environment memory-ram-critical-low
snmp-server enable traps environment memory-ram-low
snmp-server enable traps environment cpu-load
snmp-server enable traps environment cpu-critical-temp
snmp-server enable traps environment cpu-overheat-temp
snmp-server enable traps environment cpu-supercooling-temp
snmp-server enable traps file-operations
snmp-server enable traps file-operations successful
snmp-server enable traps file-operations failed
snmp-server enable traps file-operations canceled
snmp-server enable traps interfaces
snmp-server enable traps interfaces rx-utilization-high
snmp-server enable traps interfaces tx-utilization-high
snmp-server enable traps interfaces number-high
snmp-server enable traps bras
snmp-server enable traps bras sessions-number-high
snmp-server enable traps screen
snmp-server enable traps screen dest-limit
snmp-server enable traps screen source-limit
snmp-server enable traps screen icmp-threshold
snmp-server enable traps screen udp-threshold
snmp-server enable traps screen syn-flood
snmp-server enable traps screen land
snmp-server enable traps screen winnuke
snmp-server enable traps screen icmp-frag
snmp-server enable traps screen udp-frag
snmp-server enable traps screen icmp-large
snmp-server enable traps screen syn-frag
snmp-server enable traps screen unknown-proto
snmp-server enable traps screen ip-frag
snmp-server enable traps screen port-scan
snmp-server enable traps screen ip-sweep
snmp-server enable traps screen syn-fin
snmp-server enable traps screen fin-no-ack
snmp-server enable traps screen no-flag
snmp-server enable traps screen spoofing
snmp-server enable traps screen reserved
snmp-server enable traps screen quench
snmp-server enable traps screen echo-request
snmp-server enable traps screen time-exceeded
snmp-server enable traps screen unreachable
snmp-server enable traps screen tcp-all-flags
snmp-server enable traps entity
snmp-server enable traps entity config-change
snmp-server enable traps entity-sensor
snmp-server enable traps entity-sensor threshold
snmp-server enable traps envmon
snmp-server enable traps envmon shutdown
snmp-server enable traps envmon temperature
snmp-server enable traps flash
snmp-server enable traps flash insertion
snmp-server enable traps flash removal
snmp-server enable traps snmp
snmp-server enable traps snmp authentication
snmp-server enable traps snmp coldstart
```

```
bridge 1
  security-zone trusted
  ip address dhcp
  ip dhcp client ignore dns-nameserver
  ip dhcp client ignore router
  enable
exit
bridge 2
  vlan 701
  security-zone user
  ip address 198.19.253.1/24
  service-subscriber-control any
  location SSID12
  enable
exit

interface gigabitethernet 1/0/1
  description "UPLink"
  ip address dhcp
  security-zone untrusted
  service-policy dynamic all
exit
interface gigabitethernet 1/0/2.702
  bridge-group 2
exit
interface gigabitethernet 1/0/3
  mode switchport
  switchport access vlan 701
exit
interface gigabitethernet 1/0/4
  shutdown
exit
interface gigabitethernet 1/0/5
  shutdown
exit
interface gigabitethernet 1/0/6
  shutdown
exit
interface loopback 1
exit
tunnel gre 1
  keepalive retries 3
  keepalive dhcp dependent-interface bridge 1
  keepalive dhcp dependent-interface gi1/0/1
  mode ethernet
  local address xauth ipsec_vpn
  remote address xauth ipsec_vpn management-ip
  enable
exit
tunnel gre 1.1
  bridge-group 1
  snmp init-trap
  enable
exit

security zone-pair untrusted self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair trusted self
  rule 1
    action permit
    enable
  exit
exit
security zone-pair user untrusted
  rule 10
    action permit
    enable
  exit
exit
security zone-pair user self
  rule 10
    action permit
    match protocol udp
```

```
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
  exit
  rule 20
    action permit
    match protocol tcp
    match destination-port redirect
    enable
  exit
  rule 30
    action permit
    match protocol udp
    match destination-port dns
    enable
  exit
exit

access profile acc_p
exit

security ike proposal ike_prop
exit

security ike policy ike_pol
  authentication method xauth-psk-key
  authentication mode client
  proposal ike_prop
exit

security ike gateway ike_gw
  ike-policy ike_pol
  assign-interface loopback 1
  local interface gigabitethernet 1/0/1
  remote network dynamic client
  mode policy-based
  dead-peer-detection action restart
  dead-peer-detection interval 10
  dead-peer-detection timeout 60
exit

security ipsec proposal ipsec_prop
exit

security ipsec policy ipsec_pol
  proposal ipsec_prop
exit

security ipsec vpn ipsec_vpn
  mode ike
  ike establish-tunnel immediate
  ike gateway ike_gw
  ike ipsec-policy ipsec_pol
  enable
exit

nat source
  ruleset NAT
    to interface gigabitethernet 1/0/1
    rule 10
      match source-address natpool
      action source-nat interface
      enable
    exit
  exit
exit

ip dhcp-server
ip dhcp-server pool lan
  network 198.19.253.0/24
  max-lease-time 000:00:20
  default-lease-time 000:00:10
  address-range 198.19.253.2-198.19.253.254
  default-router 198.19.253.1
  dns-server 198.19.253.1
exit

ip telnet server
ip ssh server
```

clock timezone gmt +7

ntp enable
ntp server 192.168.42.178
exit

, ESR-10 -

OTT ESR-10 SA. 5 , wait-timer. , SA.

0	, SA
3	IPsec, , - IPsec SA
16	wait-timer, 43 15 , GRE keepalive dst-address
17	"OTT " , SA