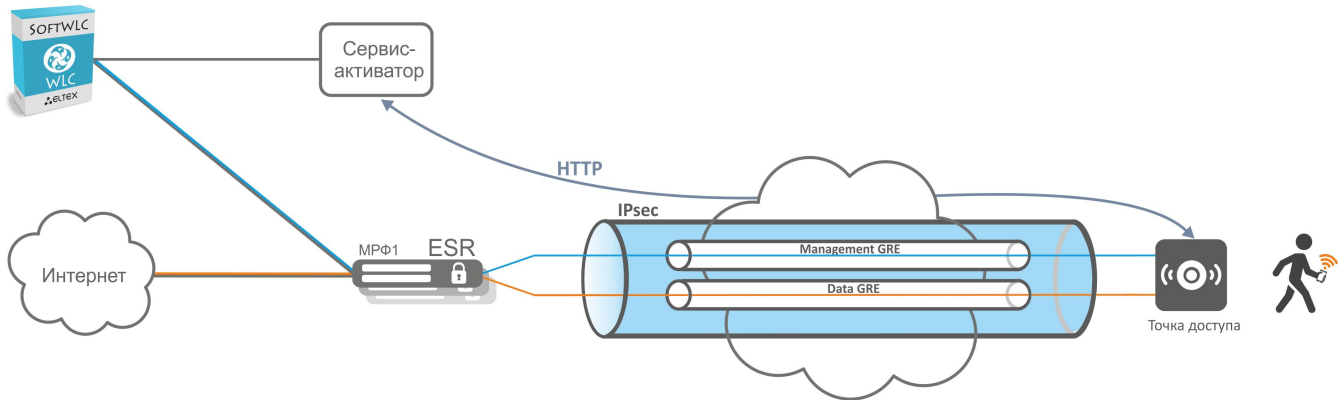


v1.17_OTT

- [illegible]



Quickstart

- ```

1. SoftWLC -:
2. /etc/eltex-wifi-sa/factory-fw.conf , () . downgrade false. /var/lib/eltex-wifi-sa/firmware/ , /etc/eltex-wifi-sa/factory-fw.conf.
3. /etc/eltex-wifi-sa/ -.
4. /etc/eltex-wifi-sa/application.conf -. CheckMAC yes. -:
service eltex-wifi-sa restart.
5. ESR .
6. . SNMP TCP .(.)
7. . "Connected".(.)
8. OTT IPsec. "IPsec password" , ESR, "testing123". NBI – CreateOttProfile.(. ESR OTT)
9. EMS ESR . OTT: ServiceProvider BRAS., ESR SoftWLC.(. ESR OTT)
10. NAS (Radius -) RADIUS ESR, , "testing123".
11. ESR OTT IP ESR OTT. NBI – CreateOttStation.(. ESR OTT)
12. SSID. SSID Location, ESR, "testing2".(.)
13. "" " " , . ()
14. " " SSID.()

```

```


-
-- x86, Ubuntu 14.04 . POST HTTPs , SoftWLC. -- WEB- . - 8043 IP- . - URL, IP- - DNS- . - EMS, SoftWLC.
- EMS (firewall). - SoftWLC firewall 8080 (HTTP), - EMS.

- -c IP- ., -c POST- - TCP- . - TCP-, .

, HTTPs- - , - . - , Provider-ID. Provider-ID - . , , , - . - MAC- , MAC- . . , handshake .. , - . /etc/eltex-
wifi-sa/factory-fw.conf. - , , - . - .

- , -, . , , - "" .

```

 () . , , -.

2 :

1. **OTT.** IPsec, ESR IPsec-.  
1. NBI [CreateOttProfile](#).
2. **OTT ESR.** IP- ESR , . IPsec OTT ESR. , -, ESR, IP- IPsec, ESR. , ESR IPsec. ESR IPsec, . OTT ESR  
NBI [CreateOttStation](#).

OTT ESR - ESR , ESR EMS. ( Service Provider), ESR . , IP- ESR , OTT. , ESR.

, , MAC. OTT Connected. , ESR OTT .

- ESR, IPsec :- ESR OTT , . ESR , , OTT ESR. OTT ESR , - 4022. ESR - , . - X-Auth , IP  
ESR, IPsec, ESR, / X-Auth.

 , , ESR. ESR, , , ESR, .

```

.

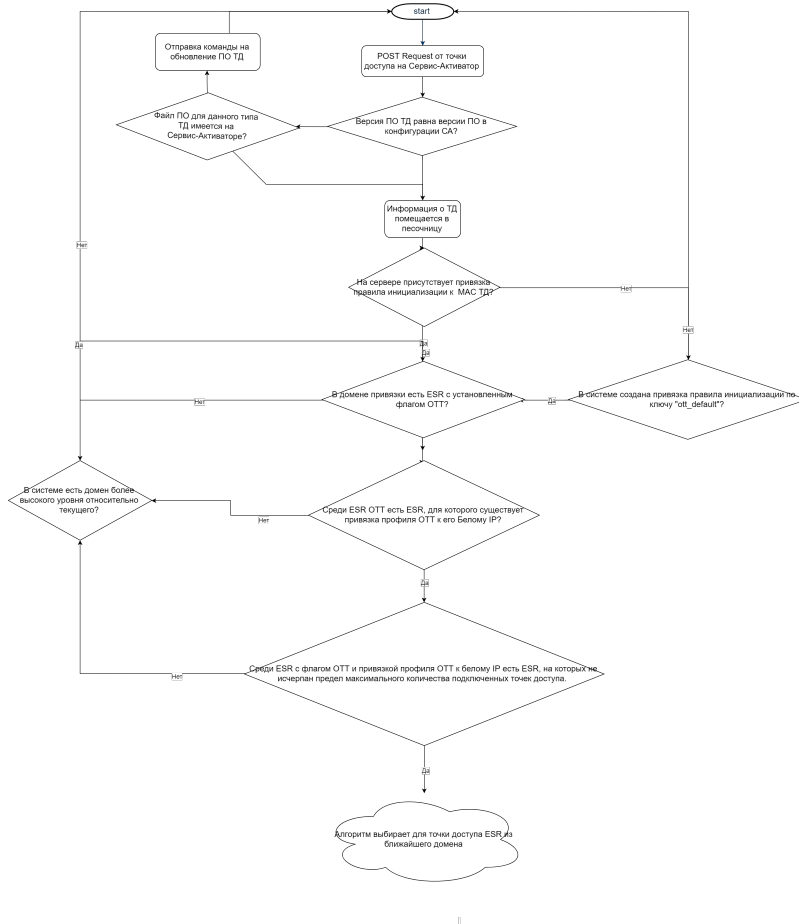
- . Wi-Fi . "ott.root" "ott_default" "ott.root". SSID . SSID , , , . ESR OTT OTT.

:

• POST- - .
• -, MAC- ESR .
• , IPsec-.
• SoftWLC, SSID, .

```

 , MA, . , , -, . - . MAC , . .



- "/etc/eltex-wifi-sa/" - : "service eltex-wifi-sa restart".

, :

"application.conf".

..

| logLevel                      | debug, info, warn, error | info       | . /var/log/eltex-wifi-sa/main.log. |
|-------------------------------|--------------------------|------------|------------------------------------|
| requestTimeout                | integer                  | 45         | M (0 ).                            |
| http { enabled                | yes, no                  | true       | HTTP.                              |
| http { port                   | integer (0-65535)        | 8042       | TCP, - HTTP.                       |
| https { enabled               | yes, no                  | true       | HTTP.                              |
| https { port                  | integer (0-65535)        | 8043       | TCP, - HTTPS.                      |
| https { keyStore { path       | string                   | server.p12 | .. , , .                           |
| https { keyStore { password   | string                   | ""         | .. - .                             |
| https { clients { certificate | string                   | client.crt | . , , .                            |
| https { clients { checkMAC    | yes, no                  | yes        | MAC- , .                           |
| https { clients { fwCheckCrt  | yes, no                  | yes        | ProviderID , .                     |
| ems { host                    | localhost IP             |            | EMS-, -.                           |

|                               |                      |      |           |
|-------------------------------|----------------------|------|-----------|
| ems { port                    | integer<br>(0-65535) | 8080 | , - EMS.  |
| ems { parallelLimit           | integer              | 5    | EMS-      |
| ipsec-activator { wait-timer  | integer              | 180  | , IPsec-. |
| ipsec-activator { update-time | integer              | 600  | , -. .    |

"factory-fw.conf"

|           |             |       |                                    |
|-----------|-------------|-------|------------------------------------|
|           |             |       |                                    |
| downgrade | true, false | false | \ ,                                |
| min       | string      |       | ,                                  |
| file      | string      |       | , /var/lib/eltex-wifi-sa/firmware/ |

/usr/lib/eltex-radius-nbi/conf/ott/ott.xml

, ESR. - , - ESR OTT , . , ESR, - ESR , ESR.

|                                         |                            |  |                                                      |
|-----------------------------------------|----------------------------|--|------------------------------------------------------|
|                                         |                            |  |                                                      |
| subtype                                 | 100, 200, 1000, 1200, 1700 |  | ESR (ESR-100, ESR-200, ESR-1000, ESR-1200, ESR-1700) |
| max                                     |                            |  | ESR                                                  |
| param name, default, regex, description |                            |  | , , , .                                              |

-.

- CPU 2 Core
- RAM 8GB
- HDD 100GB ( 5000 )

-

root@vagrant-ubuntu-trusty-64:/home/vagrant# echo "deb http://archive.eltex.org/ems 3.13 main" >> /etc/apt/sources.list.d/eltex.list

root@vagrant-ubuntu-trusty-64:/home/vagrant# add-apt-repository -y ppa:webupd8team/java

root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-key adv --keyserver keyserver.ubuntu.com --recv F558A287

root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get update

root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get -y install oracle-java8-installer

root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get install eltex-wifi-sa

, - , /etc/eltex-wifi-sa/application.conf EMS -:

```
ems {
 host = "localhost"
 port = 8080
```

## ESR

ESR 2 . , Default Gateway, ESR IPsec. ESR IP-. IP- IPsec, 500 4500 . ESR , . , 2 , Next-Hop Bridge, , Bridge, , Next-Hop Default Gateway.

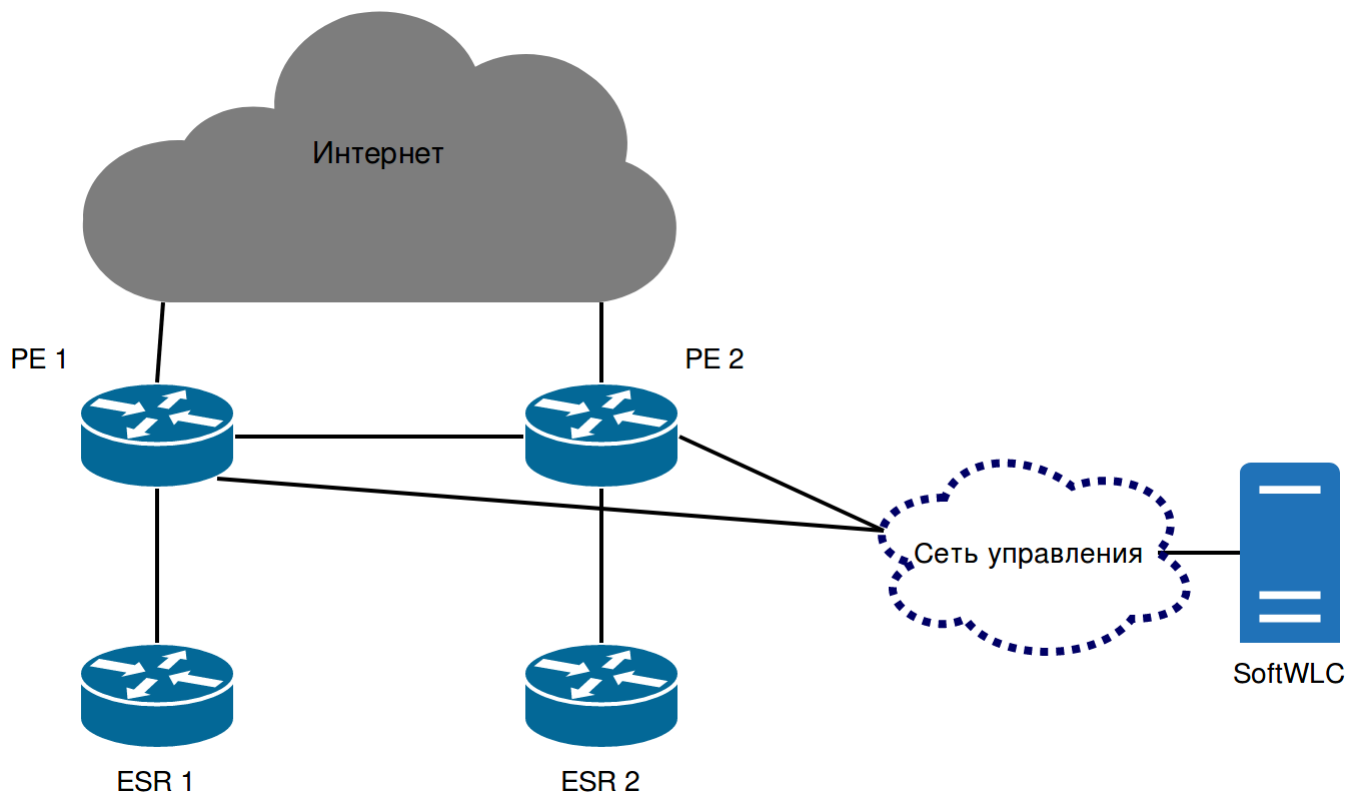
IPsec X-Auth . ESR ( - ) RADIUS- PCRF SoftWLC. PCRF Mongo DB ESR .

ESR N+1. ESR IPsec- - ESR.- ESR . ESR . ESR .

ESR -, C- ESR , . ESR ESR, - . ESR, .. ESR . ESR. , ESR . OTT ESR. ESR - , ESR. , ESR , . ESR OTT IPsec, ,.. - IPsec, ESR, .

### ESR





1. ESR 1 ESR 2, IPsec, PE 1, PE 2.
2. ESR 1, ESR 2, IPsec, BGP, PE 1 PE 2.
3. PE 1, PE 2, SoftWLC.
4. ESR, IPsec, ESR.
5. ESR IP WiFi.

ESR 3.

-, IPsec IPsec-, HTTPs, URL-, :

- 1) "Provider-ID", URL-, URL - URL - "Provider-ID", - , - , , .
  - 2) Provider-ID, Provider-ID = "eltex" URL -. URL - , - OTT . URL - CLI WEB- . - Provider-ID = "eltex". Provider-ID - , URL , , "" . "" .
- MAC- . - MAC, MAC . , - . MAC.



, . , , , , .



(URL - ), IP- DHCP 43 DHCP, . .

ESR-1000 - :

(GRE\_ping\_counter x 10) + waite\_timer,

GRE\_ping\_counter - , waite\_timer - .

310 + 180 = 210 .

1) Eltex , . URL - .- SoftWLC. IP- , DNS .

2) IP- DHCP, . DHCP 43, , IPsec . 43 . 43, .

3) HTTPs - :

- 
- MAC-
- 
- HW
- Provider-ID ( )
- MAC- ( )

4) -, , Provider-ID MAC handshake, NBI EMS, .

5) :

- MAC- , : .
- OTT, EMS "" . , .
- OTT, , , MAC, OTT - .
- , "" .

6) IPsec-, EMS MAC-.  
OTT , , . EMS - OTT . , .

7) EMS, , :

- , ESR-1000., EMS ESR-1000 IP-.
- EMS - IPsec- (MongoDB ott.xauth ).
- -, EMS : IP- ESR, (x-auth), ( ESR-1000 , IPsec-), IPsec ESR.
- - .

8) , IPsec- ESR-1000. IPsec- ESR-1000 PCRF SoftWLC. PCRF ott , , . , RADIUS access-accept.

IPsec IP- IPsec- . IP- EoGRE (Management Data) ESR-1000 IPsec .



, RADIUS :

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# mongo
> show databases;
local 0.078125GB
notification-gw 0.203125GB
ott 0.203125GB
pcrf 0.453125GB
wifi-customer-cab 0.203125GB
> use ott

> show tables

system.indexes

xauth

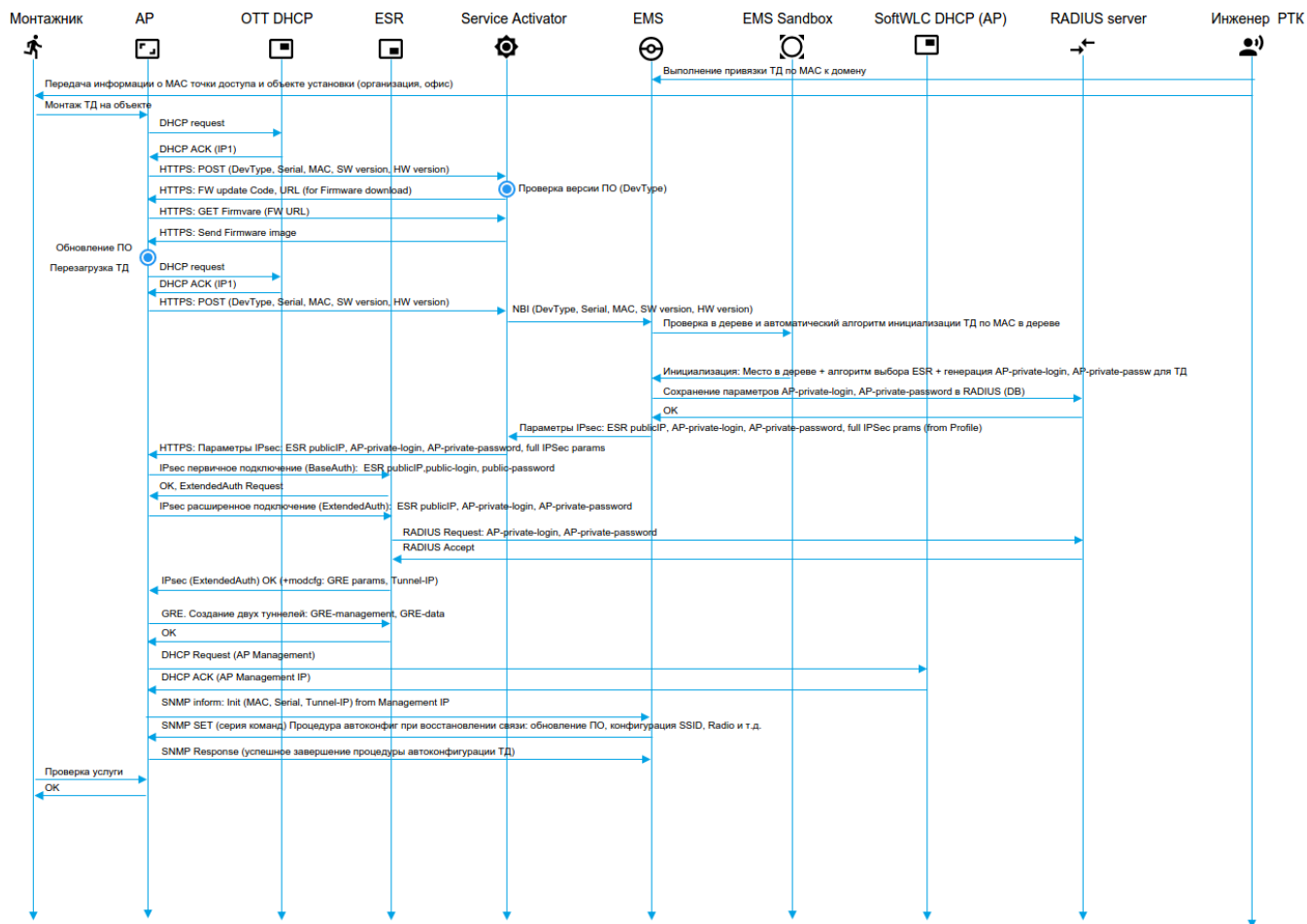
> db.xauth.find()

{ "_id" : ObjectId("5a6816b4e14c08c4d9c0854d"), "ipsec_login" : "login1", "ipsec_pass" : "password1" }
{ "_id" : ObjectId("5a6816b4e14c08c4d9c0854e"), "ipsec_login" : "login2", "ipsec_pass" : "password2" }
{ "_id" : ObjectId("5a6816b4e14c08c4d9c0854f"), "ipsec_login" : "login3", "ipsec_pass" : "password3" }
```

9) SoftWLC SNMP Management GRE , .

10) Data GRE ESR-1000 NAT.

# Инициализация ТД Элтекс в сетях сторонних операторов (ОТТ). Сценарий предконфигурации



, OTT, ott.root EMS.

ott( Wireless/ ). ott . \_SNMP\_TCP.



✕

□

Правило инициализации ТД

Главное

Тип устройства

★ WEP-12ac

Имя правила

★ ott

Домен правила

★ ott.root

🌐

Описание

RADIUS

Добавить ТД в RADIUS

☒

Ключ

★ eltex

Обновление ПО

Обновить на актуальный файл ПО

☐

Протокол загрузки ПО

TFTP

▼

Конфигурация

Восстановить конфигурацию по умолчанию

☐

Шаблон конфигурации

<Пусто>

▼

Доступ

SNMP транспорт

TCP

▼

SNMP Community (только чтение)

★ public

SNMP Community (чтение/запись)

★ private

✓ Принять

✕ Отменить

ott\_default, ott ott.root.

✕

□

Редактирование объекта

Имя устройства

WEP-12ac

Ключ

★ ott\_default

?

Имя правила

★ ott

←

Домен правила

ott.root

⦿

Домен узла

★ root

🌐

OTT (Over-the-top)

☒

✓ Принять

✕ Отменить

ott\_default , ?

**Справка**

|                          |                                                                                                        |
|--------------------------|--------------------------------------------------------------------------------------------------------|
| 0 15 10 ** ? 2005        | Ежедневно в 10:15 в течение 2005 года                                                                  |
| 0 * 14 ** ?              | Ежедневно каждую минуту с 14 до 14:59                                                                  |
| 0 0/5 14 ** ?            | Ежедневно каждые 5 минут в период с 14:00 по 14:55                                                     |
| 0 0/5 14,18 ** ?         | Ежедневно каждые 5 минут в период с 14:00 по 14:55 и с 18:00 по 18:55                                  |
| 0 0-5 14 ** ?            | Ежедневно каждую минуту в период с 14:00 по 14:05                                                      |
| 0 10,44 14 ? 3 WED       | Каждую среду в Марте в 14:10 и в 14:44                                                                 |
| 0 15 10 ? * MON-FRI      | В 10:15 каждый рабочий день (с понедельника по пятницу, вкл)                                           |
| 0 15 10 15 * ?           | В 10:15 15-го числа каждого месяца.                                                                    |
| 0 15 10 L * ?            | В 10:15 в последний день каждого месяца.                                                               |
| 0 15 10 ? * 6L           | В 10:15 в последнюю Пятницу каждого месяца. (6 - т.к. неделя у них начинается с воскресенья - номер 1) |
| 0 15 10 ? * 6L 2002-2005 | С 2002 по 2005 год в 10:15 в последнюю Пятницу каждого месяца.                                         |
| 0 15 10 ? * 6#3          | В 10:15 в третью Пятницу каждого месяца.                                                               |

**Ключ инициализации**

В поле могут быть указаны ключи для поиска привязки инициализации различного формата:

- MAC адрес - a0:b1:c2:33:44:55
- IP адрес - 1.2.3.4
- домен - sibir.root
- специальный ключ 'ott\_default' для создания привязки для ТД ОТТ по умолчанию (для любого MAC)

**✖ Закрыть**

Wireless/ .

Менеджер правил инициализации ТД

Правила  
Привязки  
ОТТ профили  
ОТТ привязки  
Черный список ОТТ

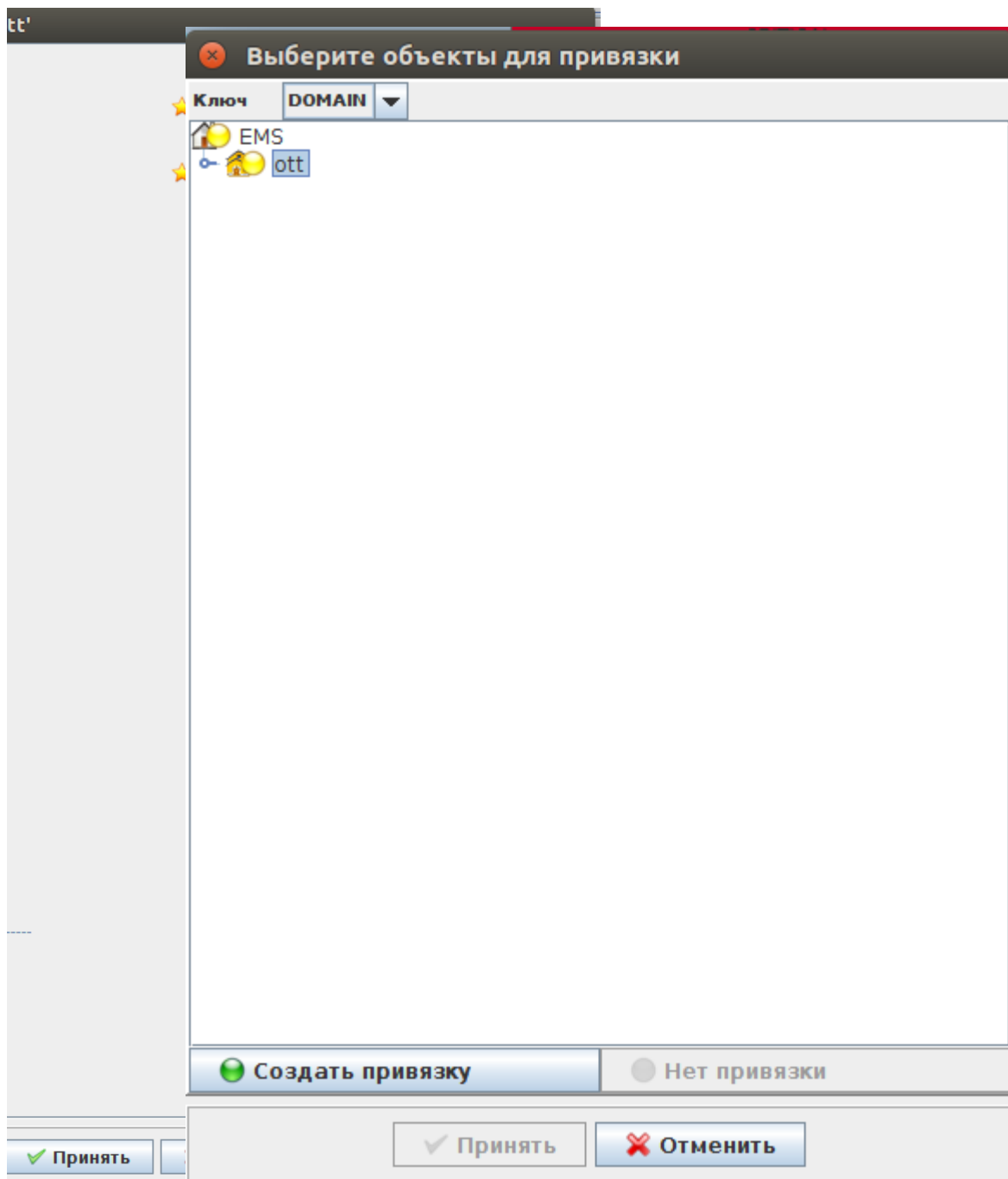
Страница: 0 / 0 на странице: 20 Фильтр:

Фильтр по домену

Изменить поля Обновить Удалить

| MAC | IP | AP Domain | Key |
|-----|----|-----------|-----|
|-----|----|-----------|-----|

SSID ott.root (Wireless/ SSID). *Bridge, Location* location, bridge ESR.



## ESR OTT

: *ServiceProvider* BRAS, *BRAS* ESR, .

Редактировать 'Доступ'

|                               |                                     |
|-------------------------------|-------------------------------------|
| Описание                      | нет                                 |
| IP адрес                      | 192.168.51.10                       |
| SNMP порт                     | 161                                 |
| SNMP транспорт                | UDP                                 |
| Файловый протокол             | TFTP                                |
| Таймаут обмена, мс            | 60000                               |
| Read community / User v3      | public                              |
| Write community / Password v3 | private                             |
| Версия SNMP                   | v2c                                 |
| Регистрация трапов            | Accept                              |
| Выведено из обслуживания      | <input type="checkbox"/>            |
| Telnet/SSH login              |                                     |
| Telnet/SSH password           |                                     |
| SSH порт                      | 22                                  |
| MAC адрес                     |                                     |
| BRAS сервис                   | <input checked="" type="checkbox"/> |
| Режим ESR                     | Station                             |
| OTT (Over-the-top)            | ServiceProvider                     |
| Дата инициализации устройства | 15.02.2018 09:59:59                 |

Принять

Отменить

IPsec ESR. ESR.

, Wireless/ OTT profiles. , 

Добавить

Менеджер правил инициализации ТД

Правила  
Привязки  
OTT profiles

Обновить Редактировать Profile

Добавить Удалить

Profile \*

----- IKE proposal -----

IKE authentication algorithm md5

IKE DH Group 1

IKE encryption algorithm aes

----- IKE policy -----

Use ISAKMP mode config UP

Use XAUTH password as IPsec password off

IKE lifetime 86400

Use NAT-T UP

IPsec NAT Keepalive 30

IPsec password

----- IPsec proposal -----

IPsec authentication algorithm md5

IPsec DH Group 0

IPsec encryption algorithm aes

----- IPsec policy -----

IPsec DPD Delay 60

IPsec child SA lifetime 3600

----- IPsec VPN -----

Force establish tunnel UP

IPsec operational status UP

----- GRE over IPSEC -----


Use GRE mode UP

GRE MTU offset 148

GRE ping counter 3

Заккрыть

, , ESR. EMS ESR .

| Описание                                                                                                                                                                                   | Мониторинг | Конфигурация | Доступ |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|--------------|--------|
| <div><div><div>Firmware</div><div>CLI/telnet</div><div>CLI/ssh</div><div>ОТТ</div></div><div></div></div> |            |              |        |
| <div>Обновить Редактировать</div>                                                                                                                                                          |            |              |        |
| <div>Добавить станцию ОТТ</div>                                                                                                                                                            |            |              |        |
| <div>Profile * <div></div></div>                                                                                                                                                           |            |              |        |
| <div>IKE gateway</div>                                                                                                                                                                     |            |              |        |
| <div>IPsec remote gateway * <div></div></div>                                                                                                                                              |            |              |        |
| <div>IKE proposal</div>                                                                                                                                                                    |            |              |        |
| <div>IKE authentication algorithm <input type="checkbox"/> md5</div>                                                                                                                       |            |              |        |
| <div>IKE DH Group <input type="checkbox"/> 1</div>                                                                                                                                         |            |              |        |
| <div>IKE encryption algorithm <input type="checkbox"/> aes</div>                                                                                                                           |            |              |        |
| <div>IKE policy</div>                                                                                                                                                                      |            |              |        |
| <div>IKE lifetime <input type="checkbox"/> 86400</div>                                                                                                                                     |            |              |        |
| <div>Use NAT-T <input type="checkbox"/> UP</div>                                                                                                                                           |            |              |        |
| <div>IPsec NAT Keepalive <input type="checkbox"/> 30</div>                                                                                                                                 |            |              |        |
| <div>IPsec password <input type="checkbox"/> <div></div></div>                                                                                                                             |            |              |        |
| <div>IPsec proposal</div>                                                                                                                                                                  |            |              |        |
| <div>IPsec authentication algorithm <input type="checkbox"/> md5</div>                                                                                                                     |            |              |        |
| <div>IPsec encryption algorithm <input type="checkbox"/> aes</div>                                                                                                                         |            |              |        |
| <div>IPsec policy</div>                                                                                                                                                                    |            |              |        |
| <div>IPsec DPD Delay <input type="checkbox"/> 60</div>                                                                                                                                     |            |              |        |
| <div>IPsec child SA lifetime <input type="checkbox"/> 3600</div>                                                                                                                           |            |              |        |
| <div>GRE over IPSEC</div>                                                                                                                                                                  |            |              |        |
| <div>GRE MTU offset <input type="checkbox"/> 148</div>                                                                                                                                     |            |              |        |
| <div>GRE ping counter <input type="checkbox"/> 3</div>                                                                                                                                     |            |              |        |

, . , IP- ESR. IPsec remote gateway , . ESR .

✖

🔍

Редактировать 'ОТТ'

Profile

\*

ott

▼

----- IKE gateway -----

Ipssec remote gateway

\*

192.168.51.10

----- IKE proposal -----

IKE authentication algorithm

☐

md5

▼

IKE DH Group

☐

1

▼

IKE encryption algorithm

☐

aes

▼

----- IKE policy -----

IKE lifetime

☐

86400

Use NAT-T

☐

UP

▼

Ipssec NAT Keepalive

☐

30

Ipssec password

☐

----- IPsec proposal -----

IPsec authentication algorithm

☐

md5

▼

IPsec encryption algorithm

☐

aes

▼

----- IPsec policy -----

IPsec DPD Delay

☐

60

IPsec child SA lifetime

☐

3600

----- GRE over IPSEC -----

GRE MTU offset

☐

148

GRE ping counter

☐

3

✓ Принять

✗ Отменить

IPsec , -

WEB- , Manage/OTT Settings

## OTT Settings

IPsec Remote Gateway  (xxx.xxx.xxx.xxx / Domain name)

IPsec Operational Status ☐

XAUTH User  (Range: 4-16 chars)

XAUTH Password  (Range: 8-48 chars)

Advanced Settings

Click "Update" to save the new settings.

IPsec, XAUTH ( , XAUTH IPsec).



Use XAUTH Password, XAUTH IPsec. IPsec Password .

Advanced Settings, IPsec



IPsec Remote Gateway  (xxx.xxx.xxx.xxx / Domain name)

IPsec Operational Status ☐

XAUTH User  (Range: 4-16 chars)

XAUTH Password  (Range: 8-48 chars)

Advanced Settings ☐

### IKE Proposal

IKE Authentication Algorithm

IKE DH Group

IKE Encryption Algorithm

### IKE Policy

Use ISAKMP Mode Config ☒ On ☐ Off

IKE Lifetime  (Sec, Range: 180-86400)

Use NAT-T ☒

IPsec NAT Keepalive  (Sec, Range: 1-300)

IPsec Password  (Range: 8-48 chars)

☒ Use XAUTH Password

### IPsec Proposal

IPsec Authentication Algorithm

IPsec DH Group

IPsec Encryption Algorithm

### IPsec Policy

IPsec DPD Delay  (Sec, Range: 5-600)

IPsec Child SA Lifetime  (Sec, Range: 180-86400)

### IPsec VPN

Force Establish Tunnel ☒

### GRE Over IPsec

Use GRE Mode ☒ On ☐ Off

GRE Over IPsec Mgmt  (xxx.xxx.xxx.xxx)

GRE Over IPsec Data  (xxx.xxx.xxx.xxx)

GRE MTU Offset  (Range: 0-220)

GRE Ping Counter  (Range: 3-60)

Click "Update" to save the new settings.

Use ISAKMP Mode Config ☒ On, GRE Over IPsec Mgmt GRE Over IPsec Data . Use ISAKMP Mode Config ☐ Off, IKE Gateway GRE Over IPsec Mgmt GRE Over IPsec Data.

IPsec Remote Gateway  (xxx.xxx.xxx.xxx / Domain name)

IPsec Operational Status ☐

Advanced Settings ☐

### **IKE Proposal**

IKE Authentication Algorithm

IKE DH Group

IKE Encryption Algorithm

### **IKE Policy**

Use ISAKMP Mode Config ☐ On ☒ Off

IKE Lifetime  (Sec, Range: 180-86400)

Use NAT-T ☒

IPsec NAT Keepalive  (Sec, Range: 1-300)

IPsec Password  (Range: 8-48 chars)

### **IKE Gateway**

IPsec Local Address  (xxx.xxx.xxx.xxx)

IPsec Remote Network  (xxx.xxx.xxx.xxx)

IPsec Remote Mask  (xxx.xxx.xxx.xxx)

### **IPsec Proposal**

IPsec Authentication Algorithm

IPsec DH Group

IPsec Encryption Algorithm

### **IPsec Policy**

IPsec DPD Delay  (Sec, Range: 5-600)

IPsec Child SA Lifetime  (Sec, Range: 180-86400)

### **IPsec VPN**

Force Establish Tunnel ☒

### **GRE Over IPsec**

Use GRE Mode ☒ On ☐ Off

GRE Over IPsec Mgmt  (xxx.xxx.xxx.xxx)

GRE Over IPsec Data  (xxx.xxx.xxx.xxx)

GRE MTU Offset  (Range: 0-220)

GRE Ping Counter  (Range: 3-60)

Click "Update" to save the new settings.

- **IPsec Remote Gateway** – IP- (xxx.xxx.xxx.xxx / ).
- **IPsec Operational Status** – IPsec.

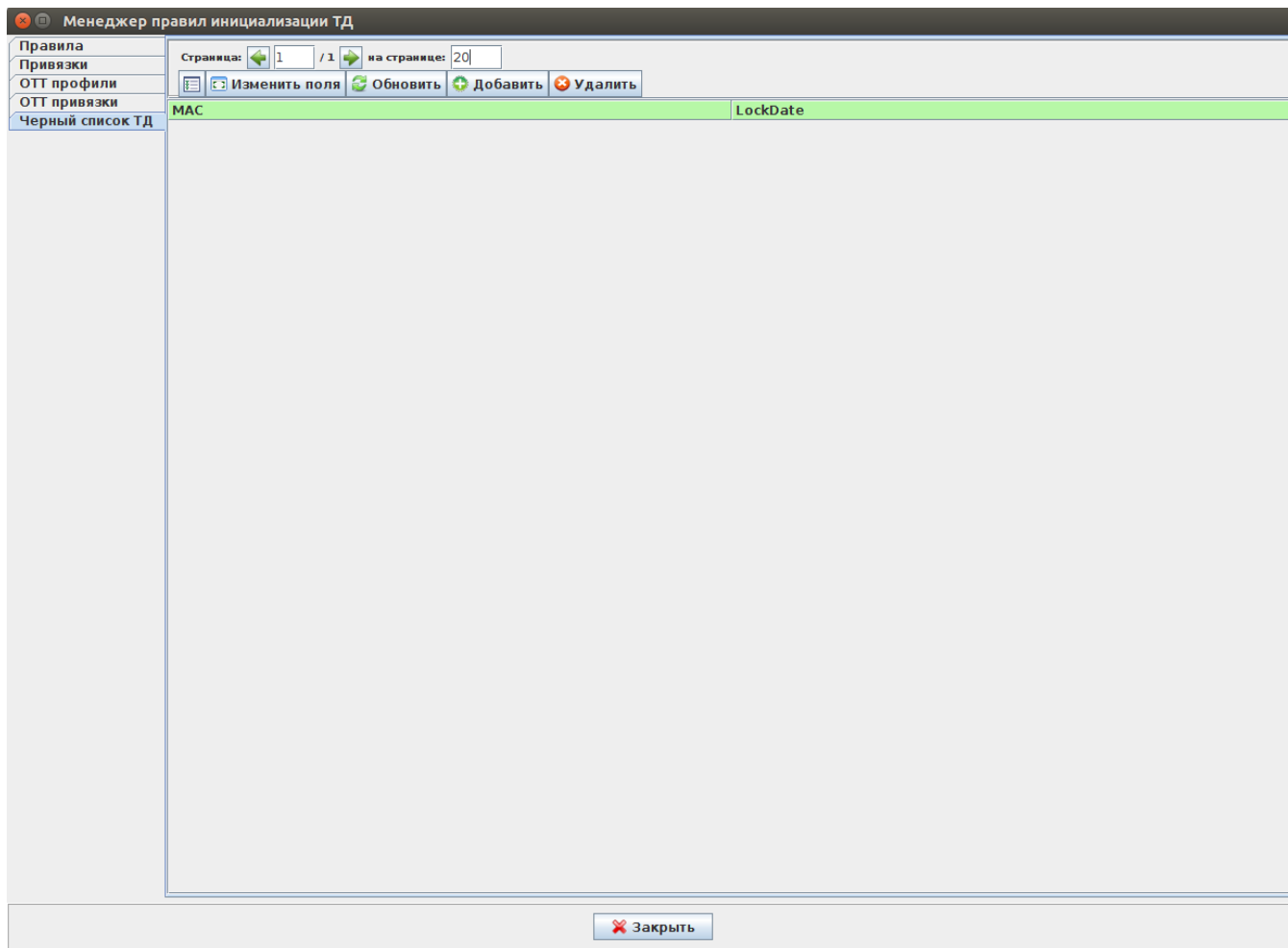
- **XAUTH User** – XAUTH, "Use ISAKMP Mode Config On" (: 4-16 ).
- **XAUTH Password** – XAUTH, "Use ISAKMP Mode Config On" (: 4-16 ).
- **IKE Authentication Algorithm** – , (md5, sha1).
- **IKE DH Group** – , (1,2,5).
- **IKE Encryption Algorithm** – 1 IPsec (AES128, DES, 3DES).
- **Use ISAKMP Mode Config** – «On» – «GRE Over IPsec Mgmt», «GRE Over IPsec Data», « IPsec», « IPsec», « IPsec Remote Mask».
- **IKE Lifetime** – IKE SA ( 1) . IKE/IPsec (, : 180–86400).
- **Use NAT-T** – , NAT.
- **IPsec NAT Keepalive** – keepalive NAT (Sec, Range: 1-300).
- **IPsec Password** – IKE/ISPEC (: 8-48 ).
- **IPsec Local Address** – , IKE 255.255.255.255 (/ 32) , « ISAKMP Config On» (xxx.xxx.xxx.xxx).
- **IPsec Remote Network** – IKE. , « ISAKMP Config On» (xxx.xxx.xxx.xxx).
- **IPsec Remote Mask** – IKE , « ISAKMP Config On» (xxx.xxx.xxx.xxx).
- **IPsec Authentication Algorithm** – , (md5, sha1).
- **IPsec DH Group** – - . 0 IKE (0,1,2,5).
- **IPsec Encryption Algorithm** – 1 IPsec (AES128, DES, 3DES).
- **IPsec DPD Delay** – ESR , (: 5-600).
- **IPsec Child SA Lifetime** – IPsec VPN SA ( 2) . **IKE/IPsec** , IKE Lifetime (Sec, Range: 180-86400).
- **Force Establish Tunnel** – GRE IPsec. IP- GRE IPsec.
- **GRE Over IPsec Mgmt** – IP- GRE (xxx.xxx.xxx.xxx).
- **GRE Over IPsec Data** – IP- GRE (xxx.xxx.xxx.xxx).
- **GRE MTU Offset** – MTU . MTU - GRE MTU Offset.
- **GRE Ping Counter** – gre-managment-ip, IPsec- . 10 . 3 60. 3.

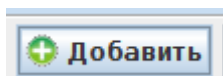


IPsec child SA lifetime IKE lifetime. . IKE lifetime 86400 (), IPsec child SA lifetime 3600 (). IPsec 24 , IKE .

GUI EMS.

Wireless/ /





MAC-

Редактирование объекта

MAC

Любое число байт MAC адреса

Принять Отменить

MAC-

, aa:bb:01, aa:bb:01:02:03:04 " aa:bb:01". , "".

## OTT link

OTT link:

- EMS
- EMS OTT,
- ESR EMS
- IP ESR EMS
- ESR EMS station
- ESR OTT

OTT:

```
$ mongo
> use ott;
> db.station.find({esr_ip: '<ip esr>'}).pretty();
```

OTT:

```
$ mongo
> use ott;
> db.xauth.find({esr_ip: '<ip esr>'}).pretty();
> db.xauth.find({mac: '<mac >'}).pretty();
```

"" " ", .

Стартовая

Статистика провайдеров

Статистика SMS

Статистика Hotspot

Статистика Enterprise

Сервисы и тарифы

Пользователи Wi-Fi

Точки доступа

Журнал событий

Беспроводные сети

Операции по расписанию

Отчеты

Конструктор порталов

Рекламная платформа

Настройки

Настройки PCRF

Система

Дерево доменов

Системные пользователи

Системные роли

Серверные адреса

RADIUS клиенты

Язык интерфейса и системных сообщений

ru\_RU

Количество неверных попыток ввода логина и пароля оператора, после которых будет произведена временная блокировка доступа по IP

10

Регулярное выражение для валидации номера телефона

^(79)(0-9){9}\$

☐ Единый домен сети

Время показа всплывающих сообщений, в сек.

2

Максимальное количество записей в Журнале событий

1000000

☒ Настройка шейперов в "Дереве доменов"

☐ Настройка CORM-2 в "Дереве доменов"

☐ Автоматическая активация ваучера при создании

Максимальное время бездействия, в мин

60

☐ Использовать кэширование в панелях статистики

Максимальное время хранения кэша на панели статистики, в мин

15

Период повторного посещения (для статистики)

12

Часы

" " SSID.

Статистика Hotspot

Статистика Enterprise

Сервисы и тарифы

Пользователи Wi-Fi

Точки доступа

Журнал событий

Беспроводные сети

Операции по расписанию

Отчеты

Конструктор порталов

Рекламная платформа

Настройки

Настройки PCRF

Справка

Правовая информация

Выход

Система

Дерево доменов

Системные пользователи

Системные роли

Серверные адреса

RADIUS клиенты

Обновить

Добавить

Редактировать

Удалить

Экспорт

Дерево доменов

| Название                      | Описание | Полный путь | Тип домена | Редактировать | Суммарный шейпер |
|-------------------------------|----------|-------------|------------|---------------|------------------|
| <input type="checkbox"/> root |          | root        | both       |               |                  |
| <input type="checkbox"/> ott  |          | ott.root    | both       |               |                  |



" " SSID.

## Суммарный shaper для 'ott.root'

×

### Домен shaper'a

ott.root

Average upstream bandwidth, Kbps

?

Peak upstream bandwidth, Kbps

?

Average downstream bandwidth, Kbps

?

Peak downstream bandwidth, Kbps

?

### Shaper'a на SSID

| SSID        | SSID domain | Average up, Kbps | Peak up, Kbps | Average down, Kbps | Peak down, Kbps |
|-------------|-------------|------------------|---------------|--------------------|-----------------|
| hotspot_ott | ott.root    |                  |               |                    |                 |

Отменить

## NBI OTT

OTT NBI.

eltex-radius-nbi. <http://localhost:8080/eltex-radius-nbi/asciidoc/>

WSDL- <http://localhost:8080/axis2/services/RadiusNbiService?wsdl>

(localhost IP- nbi)

# Описание команд NBI XML/SOAP

Система SoftWLC

---

Версия 1.9-105

Дата публикации 26-01-2018 18:14:15

[Открыть одним файлом](#)

[Введение. SoapUI](#)

1. [Управление пользователями](#)
2. [Управление тарифами](#)
3. [Управление доменами](#)
4. [Управление SSID](#)
5. [Управление устройствами](#)
6. [Управление виртуальными порталами](#)
7. [Управление системными пользователями](#)
8. [Управление шейперами](#)
9. [Управление подсетями](#)
10. [Статистика](#)
11. [Управление COPM-2](#)
12. [Управление списками URL](#)
13. [Управление списками приложений](#)
14. [Подключение ТД через сети сторонних операторов \(ОТТ\)](#)
15. [Прочие команды](#)
16. [Описание объектов и атрибутов](#)
17. [Коды ошибок](#)

## 1. IPsec

```
Description IKE authentication algorithm (md5, sha1), md5 by default
Name ipsec.auth-alg
Regex (md5|sha1)
```

```
Description IKE DH Group (1, 2, 5), 1 by default
Name ipsec.dh-group
Regex (1|2|5)
```

```
Description IPSEC DPD Delay (5..600), 60 by default
Name ipsec.dpd-delay
Regex ([5-9]|[1-9][0-9]|10[0-9]|1[1-9][0-9]|[2-5][0-9][0-9]|600)
```

```
Description IKE encryption algorithm (aes, des, 3des), aes by default
Name ipsec.encrypt-alg
Regex (aes|des|3des)
```

```
Description Force establish tunnel (UP, DOWN), UP by default
Name ipsec.force-establish
```

```

Regex (UP|DOWN)

Description Use GRE mode (UP, DOWN), UP by default
Name ipsec.gre-mode
Regex (UP|DOWN)

Description GRE mtu offset (0..220), 148 by default
Name ipsec.gre-mtu-offset
Regex ([0-9]|[1-9][0-9]|10[0-9]|1[1-9][0-9]|220|2[0-1][0-9])

Description IKE lifetime (180..86400), 86400 by default
Name ipsec.lifetime
Regex (18[0-9]|19[0-9]|[2-9][0-9][0-9]|[1-9][0-9][0-9][0-9]|1000[0-9]|100[1-9][0-9]|10[1-9][0-9][0-9]|1[1-9][0-9][0-9][0-9]|[2-7][0-9][0-9][0-9][0-9]|86400|86[0-3][0-9][0-9]|8[0-5][0-9][0-9][0-9])

Description Use ISAKMP mode config (UP, DOWN), UP by default
Name ipsec.mode-cfg
Regex (UP|DOWN)

Description Use NAT-T (UP, DOWN), UP by default
Name ipsec.nat
Regex (UP|DOWN)

Description IPSEC NAT Keepalive (1..300), 30 by default
Name ipsec.nat-keepalive
Regex ([1-9]|[1-9][0-9]|10[0-9]|1[1-9][0-9]|2[0-9][0-9]|300)

Description IPSEC password (8-48 chars)
Name ipsec.password
Regex ([A-Za-z0-9]{8,48})

Description IPSEC DH Group (0, 1, 2, 5), 0 by default
Name ipsec.pfs-group
Regex (0|1|2|5)

Description IPSEC authentication algorithm (md5, sha1), md5 by default
Name ipsec.sa-auth-alg
Regex (md5|sha1)

Description IPSEC encryption algorithm (aes, des, 3des), aes by default
Name ipsec.sa-encrypt-alg
Regex (aes|des|3des)

Description IPSEC child SA lifetime (180..86400), 3600 by default
Name ipsec.sa-lifetime
Regex (18[0-9]|19[0-9]|[2-9][0-9][0-9]|[1-9][0-9][0-9][0-9]|1000[0-9]|100[1-9][0-9]|10[1-9][0-9][0-9]|1[1-9][0-9][0-9][0-9]|[2-7][0-9][0-9][0-9][0-9]|86400|86[0-3][0-9][0-9]|8[0-5][0-9][0-9][0-9])

Description IPSEC operational status (UP, DOWN), UP by default
Name ipsec.status
Regex (UP|DOWN)

Description Use XAUTH password as IPSEC password (on/off) default off
Name ipsec.use-xauth-passwd
Regex (on|off)

Description XAUTH password (8-48 chars)
Name ipsec.xauth-password
Regex ([A-Za-z0-9]{8,48})

Description XAUTH user (4-16 chars)
Name ipsec.xauth-user
Regex ([A-Za-z0-9]{4,16})

Description IPSEC remote gateway (IP or URL)
Name ipsec.remote-gateway
<ax273:valueRegex xsi:nil="true"/>

```



2. , -

| Message                                                            |                              |
|--------------------------------------------------------------------|------------------------------|
| Connection refused                                                 | - 8042                       |
| "code":4022, "msg":"No init link found"                            |                              |
| "code":1,"msg":"In request by key 'domain' value is empty or null" | , , ESR OTT ( OTT "" )       |
| "code":4024, "msg":"No OTT station configured"                     | ESR, OTT IP- ESR OTT, ESR, . |
| "code":4023                                                        | NB                           |
| "code": 4025, "msg": "/ott/upgrade/WOP-12ac-LR-RevB.tar.gz"        | .                            |

3. ESR

ESR .

1

1.6.2, BGP, ESR, EoGRE . :

- 1) gi1/0/1.4092: 10.12.20.4/28 - , , IPsec;
  - 2) gi1/0/1.212: 100.64.0.66/30 - , VRF backbone SoftWLC, DHCP DNS ;
  - 3) gi1/0/1.213: 100.64.0.70/30 - , VRF nat ;
  - 4) bridge 1: 192.168.200.49/28 192.168.200.50/28 - EoGRE , ;
  - 5) bridge 3: 192.168.128.0/22 - . 192.168.128.1 ESR SoftWLC;
  - 6) bridge 10: 198.18.160.0/22 - . - 198.18.160.1, DNS 100.123.0.2;
  - 7) 172.31.252.0/22 - , mode config, EoGRE ;
  - 8) 100.110.123.0/24 - . 100.123.0.2 - SoftWLC, DHCP, DNS.
- .. gi1/0/1.4092, gi1/0/1.213 PBR, ESR "users\_map".

```
hostname esr-ipsec

object-group service dhcp_server
 port-range 67
exit
object-group service dhcp_client
 port-range 68
exit
object-group service ipsec_ports
 port-range 500
 port-range 4500
exit
object-group service dns
 port-range 53
exit

object-group network SoftWLC
 ip prefix 100.123.0.0/24
exit
object-group network ipsec_remote_address
 ip prefix 10.100.0.0/16
 ip prefix 172.31.252.0/22
exit
object-group network gre_termination
 ip prefix 192.168.200.48/28
exit
object-group network AP_mgmt
```

```
ip prefix 192.168.128.0/22
ip prefix 198.18.160.0/22
exit
object-group network AP_users
ip prefix 198.18.160.0/22
exit

syslog console none

radius-server timeout 10
radius-server retransmit 5
radius-server host 100.123.0.2
key ascii-text encrypted 88B11079B9014FAAF7B9
timeout 11
priority 20
source-address 192.168.128.1
auth-port 31812
acct-port 31813
retransmit 10
dead-interval 10
exit
aaa radius-profile PCRF
radius-server host 100.123.0.2
exit
das-server COA
key ascii-text encrypted 88B11079B9014FAAF7B9
port 3799
clients object-group SoftWLC
exit
aaa das-profile COA
das-server COA
exit

tech-support login enable
root login enable

vlan 3
force-up
exit
vlan 10
force-up
exit

security zone trusted
exit
security zone untrusted
exit
security zone ipsec
exit
security zone gre
exit
security zone users
exit

ip access-list extended users_pbr
rule 10
action deny
match protocol udp
match source-port 68
match destination-port 67
enable
exit
rule 11
action deny
match protocol udp
match destination-port 53
enable
exit
rule 20
action permit
enable
```

```

 exit
exit

route-map out_BGP_AP
 rule 10
 match ip address object-group AP_mgmt
 action permit
 exit
exit
route-map out_BGP_NAT
 rule 10
 match ip address object-group AP_users
 action permit
 exit
exit
route-map users_map
 rule 10
 match ip access-group users_pbr
 action set ip next-hop verify-availability 100.64.0.69 10
 action permit
 exit
exit
router bgp 64604
 address-family ipv4
 router-id 198.18.156.1
 redistribute connected
 neighbor 100.64.0.65
 remote-as 65001
 route-map out_BGP_AP out
 update-source 100.64.0.66
 enable
 exit
 neighbor 100.64.0.69
 remote-as 65001
 route-map out_BGP_NAT out
 update-source 100.64.0.70
 enable
 exit
 enable
exit
exit

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

snmp-server host 100.123.0.2
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 fan
snmp-server enable traps environment fan-speed-changed
snmp-server enable traps environment fan-speed-high
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 environment board-overheat-temp
snmp-server enable traps environment board-supercooling-temp
snmp-server enable traps wifi
snmp-server enable traps wifi wifi-tunnels-number-in-bridge-high
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 fan
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
 description "gre_termination"
 vlan 1
 security-zone gre
 ip address 192.168.200.49/28
 ip address 192.168.200.50/28
 enable
```

```
exit
```

```
bridge 3
 description "AP_mgmt"
 vlan 3
 security-zone trusted
 ip address 192.168.128.1/22
 ip helper-address 100.123.0.2
 ip tcp adjust-mss 1312
 enable
```

```
exit
```

```
bridge 10
```

```
description "Users"
vlan 10
security-zone users
ip address 198.18.160.1/22
ip helper-address 100.123.0.2
ip policy route-map users_map
ip tcp adjust-mss 1312
location data10
enable
exit

interface gigabitethernet 1/0/1
description "UpLink"
exit
interface gigabitethernet 1/0/1.212
description "VRF_backbone"
security-zone trusted
ip address 100.64.0.66/30
ip tcp adjust-mss 1312
exit
interface gigabitethernet 1/0/1.213
description "VRF_nat"
security-zone untrusted
ip address 100.64.0.70/30
ip tcp adjust-mss 1312
exit
interface gigabitethernet 1/0/1.1000
description "adm_net"
security-zone trusted
ip address 100.110.0.133/23
exit
interface gigabitethernet 1/0/1.4092
description "IPsec"
security-zone ipsec
ip address 10.12.20.4/28
exit
tunnel softgre 1
description "mgmt"
mode management
local address 192.168.200.49
default-profile
enable
exit
tunnel softgre 1.1
bridge-group 3
enable
exit
tunnel softgre 2
description "data"
mode data
local address 192.168.200.50
default-profile
enable
exit

security zone-pair trusted self
rule 10
action permit
enable
exit
exit
security zone-pair users self
rule 10
action permit
match protocol udp
match source-port dhcp_client
match destination-port dhcp_server
enable
exit
exit
security zone-pair users untrusted
```

```
rule 10
 action permit
 enable
exit
exit
security zone-pair users trusted
 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 udp
 match destination-port dns
 enable
 exit
exit
security zone-pair ipsec self
 rule 1
 action permit
 match protocol udp
 match destination-port ipsec_ports
 enable
 exit
 rule 2
 action permit
 match protocol esp
 enable
 exit
 rule 3
 action permit
 match protocol gre
 match source-address ipsec_remote_address
 match destination-address gre_termination
 enable
 exit
 rule 4
 action permit
 match protocol icmp
 enable
 exit
exit
security zone-pair trusted trusted
 rule 10
 action permit
 enable
 exit
exit

address-assignment pool ipsec_xauth_pool
 ip prefix 172.31.252.0/22
 data-tunnel address 192.168.200.50
 management-tunnel address 192.168.200.49
exit

security ike proposal dh1_md5_aes128
 authentication algorithm md5
 encryption algorithm aes128
exit

security ike policy psk_xauth
 lifetime seconds 86400
 pre-shared-key ascii-text testing123
 authentication method xauth-psk-key
 authentication mode radius
 proposal dh1_md5_aes128
exit
```

```

security ike gateway xauth_gw
 ike-policy psk_xauth
 local address 10.12.20.4
 local network 192.168.200.48/28
 remote address any
 remote network dynamic pool ipsec_xauth_pool
 mode policy-based
 dead-peer-detection action clear
 dead-peer-detection interval 60
 dead-peer-detection timeout 180
exit

security ipsec proposal md5_aes128_esp
 authentication algorithm md5
 encryption algorithm aes128
exit

security ipsec policy ipsec_pol
 proposal md5_aes128_esp
exit

security ipsec vpn xauth_ipsec
 mode ike
 ike establish-tunnel by-request
 ike gateway xauth_gw
 ike ipsec-policy ipsec_pol
 enable
exit

security passwords history 0
ip dhcp-relay

ip route 0.0.0.0/0 10.12.20.2

wireless-controller
 nas-ip-address 192.168.128.1
 resp-time 3
 failure-count 3
 data-tunnel configuration radius
 aaa das-profile COA
 aaa radius-profile PCRF
 enable
exit
ip telnet server
ip ssh server

clock timezone gmt +7

ntp enable
ntp server 100.123.0.2
exit

```

## 2

1.4.0, , ESR, EoGRE. :

- 1) bridge 1: 192.168.171/24 - , , IPsec;
- 2) bridge 2: 192.168.110.0.37/24 - , ;
- 2) bridge 3: 101.0.0.171/24 - SoftWLC, DHCP DNS. SoftWLC. SoftWLC 101.0.0.24;
- 3) bridge 5: 192.168.7.1/30 192.168.7.2.30 - EoGRE , ;
- 4) bridge 6: 172.31.239.1/26 - ;
- 5) bridge 7: 172.31.239.65/26 - ;
- 6) bridge 94: 10.12.12.1/30 - ;

7) 172.31.250.0/24 - , mode config, EoGRE .

.. bridge 1, bridge 94 PBR, ESR "clients\_br7".

```
hostname esr-ipsec

tech-support login enable
root login enable

syslog max-files 3
syslog file-size 512

object-group service telnet
 port-range 23
exit
object-group service ssh
 port-range 22
exit
object-group service dhcp_server
 port-range 67
exit
object-group service dhcp_client
 port-range 68
exit
object-group service ntp
 port-range 123
exit
object-group service ipsec_ports
 port-range 500
 port-range 4500
exit
object-group service snmp
 port-range 161-162
exit
object-group service COA
 port-range 3799
 port-range 31812-31813
 port-range 1812-1813
exit
object-group service redirect
 port-range 3128
 port-range 3129
exit

object-group network SoftWLC
 ip address-range 101.0.0.24
exit
object-group network ipsec_remote_address
 ip prefix 172.31.250.0/24
exit
object-group network gre_termination
 ip prefix 192.168.7.0/30
exit

object-group url defaultserv
 url http://eltex-co.ru
exit

-, data- .
radius-server timeout 10
radius-server retransmit 5
radius-server host 101.0.0.24
 key ascii-text testing123
 timeout 11
 priority 20
 source-address 101.0.0.171
 auth-port 31812
 acct-port 31813
```



```

 retransmit 10
 dead-interval 10
exit
aaa radius-profile PCRF
 radius-server host 101.0.0.24
exit

ESR, -.
das-server COA
 key ascii-text testing123
 port 3799
 clients object-group SoftWLC
exit
aaa das-profile COA
 das-server COA
exit

vlan 2
 force-up
exit
vlan 7
 name "mgmt"
 force-up
exit
vlan 100
 name "user"
 force-up
exit
vlan 808
 name "GRE"
 force-up
exit
vlan 1001
 name "from_SoftWLC"
 force-up
exit
vlan 1108
 force-up
exit
vlan 4094
 force-up
exit

security zone trusted
exit
security zone user
exit
security zone mgmt
exit
security zone gre
exit
security zone ipsec
exit
security zone clients_inet
exit

, , policy-based routing.
ip access-list extended users_filter
 rule 1
 action permit
 match protocol any
 match source-address 172.31.239.64 255.255.255.192
 match destination-address any
 enable
 exit
exit

#DHCP-request DHCP-, ip, SotfWLC.
ip access-list extended clients_dhcp
 rule 1
 action permit

```

```

 match protocol udp
 match source-address 172.31.239.64 255.255.255.192
 match destination-address 101.0.0.24 255.255.255.255
 match source-port 68
 match destination-port 67
 enable
 exit
exit

route-map, , .
route-map clients_br7
 rule 1 #DHCP-request DHCP .
 match ip access-group clients_dhcp
 action set ip next-hop verify-availability 101.0.0.24 10
 action permit
 exit
 rule 2 # , .
 match ip access-group users_filter
 action set ip next-hop verify-availability 10.12.12.2 10
 action permit
 exit
exit

snmp-server
snmp-server system-shutdown # ESR SNMP- EMS.
snmp-server community "private1" rw
snmp-server community "public11" ro

snmp-server host 101.0.0.24
exit

, , IPsec .
bridge 1
 vlan 1108
 security-zone ipsec
 ip address 192.168.108.171/24
 enable
exit

, .
bridge 2
 vlan 2
 security-zone trusted
 ip address 192.168.110.37/24
 enable
exit

SoftWLC.
bridge 3
 description "SoftWLC"
 vlan 1001
 security-zone mgmt
 ip address 101.0.0.171/24
 enable
exit

GRE .
bridge 5
 vlan 808
 security-zone gre
 ip address 192.168.7.1/30
 ip address 192.168.7.2/30
 enable
exit

.
bridge 6
 vlan 7
 security-zone mgmt
 ip address 172.31.239.1/26
 ip helper-address 101.0.0.24

```

```

 ip tcp adjust-mss 1312
 protected-ports
 protected-ports exclude vlan
 enable
exit

#, .
bridge 7
 vlan 100
 security-zone user
 ip address 172.31.239.65/26
 ip helper-address 101.0.0.24
 ip policy route-map clients_br7 # policy-based routing .
 ip tcp adjust-mss 1312
 location testing2
 protected-ports
 protected-ports exclude vlan
 enable
exit

#, , .
bridge 94
 vlan 4094
 security-zone clients_inet
 ip address 10.12.12.1/30
 ip tcp adjust-mss 1312
 enable
exit

interface port-channel 1
 switchport forbidden default-vlan
 switchport general acceptable-frame-type tagged-only
 switchport general allowed vlan add 2,1001,1108,4094 tagged
exit
interface gigabitethernet 1/0/1
 channel-group 1 mode auto
exit
interface gigabitethernet 1/0/2
 channel-group 1 mode auto
exit
interface gigabitethernet 1/0/3
 shutdown
 security-zone trusted
 ip firewall disable
exit
interface gigabitethernet 1/0/4
 shutdown
 security-zone trusted
 ip firewall disable
exit
interface tengigabitethernet 1/0/1
 shutdown
 ip firewall disable
 switchport forbidden default-vlan
exit
interface tengigabitethernet 1/0/2
 shutdown
 ip firewall disable
 switchport forbidden default-vlan
exit
exit
tunnel softgre 1
 description "mgmt"
 mode management
 local address 192.168.7.1
 default-profile
 enable
exit
tunnel softgre 1.1
 bridge-group 6
 enable

```

```
exit
tunnel softgre 2
 description "data"
 mode data
 local address 192.168.7.2
 default-profile
 enable
exit

security zone-pair trusted self
 rule 1
 action permit
 match protocol tcp
 match source-address any
 match destination-address any
 match source-port any
 match destination-port ssh
 enable
 exit
 rule 2
 action permit
 match protocol tcp
 match source-address any
 match destination-address any
 match source-port any
 match destination-port telnet
 enable
 exit
 rule 3
 action permit
 match protocol icmp
 match source-address SoftWLC
 match destination-address any
 enable
 exit
exit
security zone-pair user self
 rule 10
 action permit
 match protocol udp
 match source-address any
 match destination-address any
 match source-port dhcp_client
 match destination-port dhcp_server
 enable
 exit
 rule 20
 action permit
 match protocol tcp
 match source-address any
 match destination-address any
 match source-port any
 match destination-port redirect
 enable
 exit
exit
security zone-pair clients_inet self
 rule 10
 action permit
 match protocol any
 match source-address any
 match destination-address any
 exit
exit
security zone-pair user clients_inet
 rule 1
 action permit
 match protocol any
 match source-address any
 match destination-address any
 enable
```

```

 exit
exit
security zone-pair ipsec self
 rule 1
 action permit
 match protocol udp
 match source-address any
 match destination-address any
 match source-port ipsec_ports
 match destination-port ipsec_ports
 enable
 exit
 rule 2
 action permit
 match protocol esp
 match source-address any
 match destination-address any
 enable
 exit
 rule 3 #.. GRE IPSec , , .
 action permit
 match protocol gre
 match source-address ipsec_remote_address
 match destination-address gre_termination
 enable
 exit
 rule 4
 action permit
 match protocol icmp
 match source-address ipsec_remote_address
 match destination-address gre_termination
 enable
 exit
exit
security zone-pair mgmt self
 rule 1
 action permit
 match protocol tcp
 match source-address any
 match destination-address any
 match source-port any
 match destination-port ssh
 enable
 exit
 rule 2
 action permit
 match protocol tcp
 match source-address any
 match destination-address any
 match source-port any
 match destination-port telnet
 enable
 exit
 rule 3
 action permit
 match protocol icmp
 match source-address SoftWLC
 match destination-address any
 enable
 exit
 rule 4
 action permit
 match protocol udp
 match source-address SoftWLC
 match destination-address any
 match source-port any
 match destination-port snmp
 enable
 exit
 rule 5
 action permit

```

```
match protocol udp
match source-address SoftWLC
match destination-address any
match source-port any
match destination-port COA
enable
exit
rule 6
 action permit
 match protocol tcp
 match source-address SoftWLC
 match destination-address any
 match source-port any
 match destination-port COA
 enable
exit
rule 7
 action permit
 match protocol icmp
 match source-address any
 match destination-address any
 enable
exit
rule 10
 action permit
 match protocol udp
 match source-address any
 match destination-address any
 match source-port dhcp_client
 match destination-port dhcp_server
 enable
exit
rule 11
 action permit
 match protocol udp
 match source-address any
 match destination-address any
 match source-port dhcp_server
 match destination-port dhcp_server
 enable
exit
exit
security zone-pair mgmt mgmt
 rule 1
 action permit
 match protocol icmp
 match source-address any
 match destination-address any
 enable
 exit
 rule 10
 action permit
 match protocol udp
 match source-address any
 match destination-address any
 match source-port dhcp_client
 match destination-port dhcp_server
 enable
 exit
 rule 20
 action permit
 match protocol udp
 match source-address SoftWLC
 match destination-address any
 match source-port any
 match destination-port snmp
 enable
 exit
 rule 21
 action permit
 match protocol udp
```

```
match source-address any
match destination-address SoftWLC
match source-port any
match destination-port snmp
enable
exit
rule 22
 action permit
 match protocol tcp
 match source-address SoftWLC
 match destination-address any
 match source-port any
 match destination-port snmp
 enable
exit
rule 23
 action permit
 match protocol tcp
 match source-address any
 match destination-address SoftWLC
 match source-port any
 match destination-port snmp
exit
rule 30
 action permit
 match protocol tcp
 match source-address any
 match destination-address any
 match source-port any
 match destination-port telnet
 enable
exit
rule 31
 action permit
 match protocol tcp
 match source-address any
 match destination-address any
 match source-port any
 match destination-port ssh
 enable
exit
rule 49
 action permit
 match protocol udp
 match source-address any
 match destination-address SoftWLC
 match source-port any
 match destination-port ntp
 enable
exit
rule 50
 action permit
 match protocol udp
 match source-address any
 match destination-address SoftWLC
 match source-port any
 match destination-port COA
 enable
exit
exit
security zone-pair mgmt user
 rule 10
 action permit
 match protocol udp
 match source-address SoftWLC
 match destination-address any
 match source-port dhcp_server
 match destination-port dhcp_server
 enable
 exit
exit
```

```

security zone-pair gre ipsec
rule 1
 action permit
 match protocol any
 match source-address gre_termination
 match destination-address ipsec_remote_address
 enable
exit
exit

, mode config.
address-assignment pool ipsec_pool_1
ip prefix 172.31.250.0/24 # ,
ip (tunnel ip) GRE .
tunnel ip EMS.
data-tunnel address 192.168.7.2 #, GRE data .
management-tunnel address 192.168.7.1 #, GRE .
exit

IKE : MD5, - DH1, aes128.
security ike proposal dh1_md5_aes128
 authentication algorithm md5
 encryption algorithm aes128
exit

IKE.
security ike policy psk_xauth1
 lifetime seconds 86400 # ().
 pre-shared-key ascii-text testing123 #
 authentication method xauth-psk-key # XAUTH.
 authentication mode radius # - .
 proposal dh1_md5_aes128 # .
exit

, .
security ike gateway ike1_from_inet
 ike-policy psk_xauth1 # IKE.
 local address 192.168.108.171 #, IPSec .
 local network 192.168.7.0/30 # , IPSec .
 remote address any # IPSec - .
 remote network dynamic pool ipsec_pool_1 # .
 mode policy-based # policy-based
 dead-peer-detection action clear # IPSec .
 dead-peer-detection interval 60 # dead-peer-detection .
 dead-peer-detection interval 180 #, , IPSec ,
 # DPD .
exit

IPSec: MD5, AES128, ESP.
security ipsec proposal md5_aes128_esp
 authentication algorithm md5
 encryption algorithm aes128
exit

IPSec.
security ipsec policy vpn1_poll
 lifetime seconds 3600 # IPSec hald SA ().
 proposal md5_aes128_esp # IPSec, .
exit

IPSec VPN, .
security ipsec vpn for_INET_1
 mode ike # IKE.
 ike establish-tunnel by-request # IPSec .
 ike gateway ike1_from_inet # , , IKE.
 ike ipsec-policy vpn1_poll # IPSec, .
 enable
exit

ip dhcp-relay

```



```

ip route 0.0.0.0/0 192.168.108.1 200

wireless-controller
nas-ip-address 101.0.0.171
data-tunnel configuration radius # data-
aaa das-profile COA
aaa radius-profile PCRF
enable
exit
ip telnet server
ip ssh server

clock timezone gmt +7

ntp enable
ntp server 101.0.0.24
prefer
exit

```

ESR 1200/1700 1.4.1 - , EoGRE. : [ESR OTT](#) .

## Troubleshooting

- 
- `/var/log/eltex-wifi-sa/wifi-sa-server.log.` application.conf LogLevel = debug

CLI :

- :
- WEP-12ac\_rev\_C# *get ipsec-activator*

IPsec, -:

WEP-12ac\_rev\_C# *get ipsec-dynamic*

URL -, :

WEP-12ac\_rev\_C# *sh*

/mnt/root # *cd /etc/cert/*  
 /etc/cert # *cat sa-host.txt*  
<https://126.0.10.4:8043>

provider-id MAC :

WEP-12ac\_rev\_C# *sh*

/etc/cert # *openssl x509 -in /etc/cert/cert.pem -text -noout*  
 WARNING: can't open config file: /etc/pki/tls/openssl.cnf  
 Certificate:  
 Data:  
 Version: 3 (0x2)  
 Serial Number:  
 e0:d9:e3:70:1d:00:bc:2a:aa:28:54:ee:9f:27:5a:77  
 Signature Algorithm: sha256WithRSAEncryption  
 Issuer: CN=OTT Certification Root (Test), O=Eltex Enterprise Ltd., OU=Wi-Fi, C=RU, L=Novosibirsk  
 Validity  
 Not Before: Jan 1 00:00:00 1999 GMT  
 Not After : Jan 1 00:00:00 2100 GMT  
 Subject: CN=E0:D9:E3:70:1D:00, O=provider\_eltex  
 Subject Public Key Info:  
 Public Key Algorithm: rsaEncryption  
 Public-Key: (2048 bit)  
 Modulus:  
 .....

e0:d9:e3:70:1d:00 - MAC ,

provider\_eltex - Provider-ID

-

*service-activator <https://<URL>:8043> --msg-type register --timeout 300 -C /etc/cert/cert.pem -K /etc/cert/key.pem -A /etc/cert/ca.pem -d 15*

- .