AMPEC
Академска мрежа Србије

Упустсво за подешавања RADIUS сервера за иAMPEC услугу

Историја верзија документа

Верзија	Датум	Иницијали аутора	Опис промене
1.0	MAJ 2015	НИ, МВ	Прва верзија овог документа

Садржај

1 Увод

Ради реализације Даваоца идентитета за иAMPEC услугу у оквиру институције се користи постојећа RADIUS инфраструктура за аутентификацију која је имплементирана за eduroam потребе. У овом упутству, приказана је додатна конфигурација коју је потребно извршити на RADIUS серверу на институцији који је имплементиран коришћењем FreeRadius софтвера.

Како би се заштитила комуникација, односно RADIUS пакети који се размењују између иAMPEC портала и RADIUS сервера институције, неопходно је успоставити IPsec тунел. У оквиру овог упутства дате су смернице за подешавање IPsec тунела на CentOS и Debian оперативним системима.

2 Подешавање RADIUS сервера

Сви фајлови у оквиру којих је потребно унети измене се налазе у `raddb` фолдеру. У зависности од начина инсталације, `raddb` фолдер се налази у `/etc/` или `/usr/local/etc/` директоријуму.

Подешавање конфигурације на RADIUS серверу подразумева следеће кораке:

1. Креирање `iamres` виртуелног сервера

На FreeRadius платформи, креирање независних подешавања RADIUS сервера за различите намене омогућено је коришћењем тзв. виртуелних сервера. За потребе иAMPEC, неопходно је да формирате `iamres` виртуелни сервер који ће обрађивати аутентификационе захтеве који стижу са иAMPEC портала.

i. потебно је да у директоријуму `/raddb/sites-available` копирате `default` конфигурациони фајл у нови `iamres` фајл:

```
$ cp default iamres
```

ii. На почетку новог `aai` конфигурационог фајла, пре `authorize` секције, потребно је да додате „`server aai {`“ и на крају фајла затворити ову секцију са „`}`“. Такође је потребно закоментарисати `chap`, `mschap`, `digest`, `eap` и `files` модуле, а укључити (одкоментарисати) `pap` и `ldap` модуле унутар `authorize` секције.

```
server aai {
authorize {

#chap
#mschap
#digest
#eap {
#     ok = return
#     }
# files

ldap
pap
```

```
}
...
}
```

НАПОМЕНА: Уколико не користите LDAP базу за аутентификацију корисника, потребно је да уместо `ldap` модула укључите модул који одговара вашој бази.

iii. у `/raddb/sites-enabled` директоријуму, потребно је да направите нови софт линк ка iamres фајлу:

```
$ ln –s /usr/local/etc/raddb/sites-available/aai
```

2. Додавање RADIUS клијента

i. У `client.conf` фајлу потребно је да додате новог клијента на следећи начин:

```
client  iamres {
        ipaddr          = 147.91.1.11
        secret          = ******  # lozinka se dobija od AMRES-a
        shortname       = iamres
        nastype         = other
        virtual_server  = aai
}
```

3. Додавање атрибута за потребе иAMPEC

i. У `dictionary` фајлу је потребно да дефинишете атрибуте на следећи начин:

```
VENDOR          AMRES           11067

BEGIN-VENDOR AMRES

ATTRIBUTE       AMRES-Attribute-sn           1       string
ATTRIBUTE       AMRES-Attribute-gn           2       string
ATTRIBUTE       AMRES-Attribute-uid          3       string
ATTRIBUTE       AMRES-Attribute-cn           4       string
ATTRIBUTE       AMRES-Attribute-mail         5       string
ATTRIBUTE       AMRES-Attribute-o            6       string
ATTRIBUTE       AMRES-Attribute-entitlement  7       string
ATTRIBUTE       AMRES-Attribute-displayName  8       string
ATTRIBUTE    AMRES-Attribute-Affiliation  9      string

END-VENDOR AMRES
```

ii. У `ldap.attrmap` фајлу је потребно да дефинишете мапирање атрибута за потребе федерације:

```
# iamres
replyItem       AMRES-Attribute-sn              sn
replyItem       AMRES-Attribute-gn              givenName
replyItem       AMRES-Attribute-uid             uid
replyItem       AMRES-Attribute-cn              cn
replyItem       AMRES-Attribute-o               o
replyItem       AMRES-Attribute-entitlement     eduPersonEntitlement +=
replyItem       AMRES-Attribute-displayName     displayName
replyItem       AMRES-Attribute-Affiliation     rsEduPersonAffiliation
```

НАПОМЕНА: Уколико атрибут који садржи име матичне институције не постоји у LDAP бази, могуће је подесити да се овај атрибут додаје за сваког корисника. Потребно је:

- Из `ldap.attrmap` фајла да избаците линију која се односи на овај атрибут;
- У фајл `/sites-available/aai` у оквиру `post-auth` секције унесите:

```
update reply {
       AMRES-Attribute-o := "naziv institucije"
       }
```

где је "назив институције" званичан назив ваше институције.

4. Наведени атрибути у `ldap.attrmap` фајлу су глобално доступни, тачније сваки сервис дефинисан на RADIUS серверу ће, у оквиру одговарајуће RADIUS поруке, слати овај сет атрибута. Због тога је неопходно дефинисати филтрирање ових атрибута у одговарајућим фајловима осталих сервиса.

i. За `eduroam` сервис у фајлу `eduroam-inner-tunnel` у `post-auth` секцији потребно је да додате:

```
        update reply {
        Class !* ANY
        AMRES-Attribute-mail !* ANY
        AMRES-Attribute-cn !* ANY
        AMRES-Attribute-uid !* ANY
        AMRES-Attribute-gn !* ANY
        AMRES-Attribute-sn !* ANY
        AMRES-Attribute-o !* ANY
        AMRES-Attribute-entitlement !* ANY
        AMRES-Attribute-displayName !* ANY
    AMRES-Attribute- Affiliation !* ANY
        }
```

ii. За VPN сервис у фајлу `vpn` у `post-auth` секцији потребно је да додате:

```
        update reply {
        Class !* ANY
        AMRES-Attribute-mail !* ANY
        AMRES-Attribute-cn !* ANY
        AMRES-Attribute-uid !* ANY
        AMRES-Attribute-gn !* ANY
        AMRES-Attribute-sn !* ANY
        AMRES-Attribute-o !* ANY
        AMRES-Attribute-entitlement !* ANY
        AMRES-Attribute-displayName !* ANY
    AMRES-Attribute- Affiliation !* ANY
        }
```

5. Овим је завршена конфигурација RADIUS сервера. Потребно је да стартујете сервер у debug моду и проверите да ли је сервер учитао конфигурацију:

```
$ killall radiusd
$ radiusd -X
```

6. Након изласка из `debug` мода потребно је да поново покренете RADIUS сервер:

```
$ radiusd
```

3 Подешавање IPsec тунела на CentOS оперативном систему

3.1 Инсталација IPsec пакета

1. За реализацију IPsec тунела између RADIUS сервера институције и иAMPEC сервера, потребно је да на RADIUS серверу институције инсталирате следеће алате:

iii. За CentOS5 : `openswan, ipsec-tools, nss-tools, which, lsof:`

```
$ yum install openswan ipsec-tools nss-tools which lsof
```

iv. За CentOS6: `libreswan, nss-tools, which, lsof:`

```
$ yum install libreswan nss-tools which lsof
```

НАПОМЕНА: Уколико `libreswan` пакет не постоји у стандардним репозиторијумима, потребно је да инсталирате RHEL EPEL репозиторијуме на следећи начин:

```
$ wget http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-
8.noarch.rpm
$ wget http://rpms.famillecollet.com/enterprise/remi-release-6.rpm
```

```
$ sudo rpm -Uvh remi-release-6*.rpm epel-release-6*.rpm
```

Након успешне инсталације потребних репозиторијума, у директоријуму `/etc/yum.repos.d` би требало да постоје следећи фајлови:

```
/etc/yum.repos.d/epel.repo
/etc/yum.repos.d/epel-testing.repo
/etc/yum.repos.d/remi.repo
```

2. Уколико није искључен, потребно је да искључите SELINUX:

```
$ cat /etc/sysconfig/selinux
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - SELinux is fully disabled.
SELINUX=disabled
# SELINUXTYPE= type of policy in use. Possible values are:
#       targeted - Only targeted network daemons are protected.
#       strict - Full SELinux protection.
SELINUXTYPE=targeted

# SETLOCALDEFS= Check local definition changes
SETLOCALDEFS=0
```

3. Након инсталације потребно је да у `/etc/sysctl.conf` фајл унесете следеће промене (обратити пажњу да је неким променљивим потребно променити вредност, а неке је потребно додати):

```
# IPSec
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.eth0.rp_filter = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.ipv4.conf.default.log_martians = 0
net.ipv4.ip_forward = 1
```

4. Након ових промена потребно је да поново покренете `sysctl` следећом командом:

```
$ sysctl -p
```

5. Када су инсталирани сви неопходни алати могуће је покренути IPsec сервис и тестирати инсталацију, односно тестирати да ли је сервис покренут како треба:

```
$ service ipsec start
$ ipsec verify
```

Излаз команде `ipsec verify`, када је све покренуто како треба, треба да изгледа овако:

i. За CentOS5, односно Openswan:

```
Checking your system to see if IPsec got installed and started correctly:
Version check and ipsec on-path                                 [OK]
Linux Openswan U2.6.32/K2.6.32-279.5.1.el6.i686 (netkey)
Checking for IPsec support in kernel                            [OK]
 SAref kernel support                                           [N/A]
 NETKEY:  Testing for disabled ICMP send_redirects              [OK]
NETKEY detected, testing for disabled ICMP accept_redirects     [OK]
Checking that pluto is running                                  [OK]
 Pluto listening for IKE on udp 500                             [OK]
 Pluto listening for NAT-T on udp 4500                          [OK]
Checking for 'ip' command                                       [OK]
Checking /bin/sh is not /bin/dash                               [OK]
Checking for 'iptables' command                                 [OK]
Opportunistic Encryption Support                                [DISABLED]
```

ii. За CentOS6, односно Libreswan:

```
Verifying installed system and configuration files

Version check and ipsec on-path                         [OK]
Libreswan 3.7 (netkey) on 2.6.32-358.el6.i686
Checking for IPsec support in kernel                    [OK]
 NETKEY: Testing XFRM related proc values
         ICMP default/send_redirects                    [OK]
         ICMP default/accept_redirects                  [OK]
         XFRM larval drop                               [OK]
Pluto ipsec.conf syntax                                 [OK]
Hardware random device                                  [N/A]
Checking rp_filter                                      [OK]
Checking that pluto is running                          [OK]
 Pluto listening for IKE on udp 500                     [OK]
 Pluto listening for IKE/NAT-T on udp 4500              [OK]
 Pluto ipsec.secret syntax                              [OK]
Checking NAT and MASQUERADEing                          [TEST INCOMPLETE]
Checking 'ip' command                                   [OK]
```

```
Checking 'iptables' command                                [OK]
Checking 'prelink' command does not interfere with FIPSChecking for obsolete
ipsec.conf options                 [OK]
Opportunistic Encryption                                   [DISABLED]
```

6. За RADIUS сервер институције потребно је да отворите следеће портове:
   - UDP port 500 за Internet Key Exchange (IKE) протокол
   - UDP port 4500 за IKE NAT-Traversal
   - Protocol 50 за Encapsulated Security Payload (ESP) IPsec пакете

3.2 Конфигуарција IPsec тунела

Радни фолдер openswan/libreswan пакета инсталираног на начин описан у поглављу 3.1 је /etc/ipsec.d

Фајлови од значаја су главни конфигурациони фајл `/etc/ipsec.conf` и `/etc/ipsec.secret` фајл који се користи у процесу аутентификације сервера између којих се успоставља IPsec тунел. У зависности од начина аутентификације, у фајл `ipsec.secret` је потребно да поставите дељене кључеве, RSA потписе или показиваче на X.509 дигиталне сертификате.

Више информација о овим фајловима можете добити на страницам упутства за коришћење команди `ipsec.conf` и `ipsec.secrets` (коришћењем `man` команде).

1. У главном конфигурационом фајлу `/etc/ipsec.conf`, је потребно да уклоните коментар у последњој линији, испред `include /etc/ipsec.d/*.conf` како би се конфигурације конкретних IPsec тунела раздвојиле у посебне конфигурационе фајлове (који морају да се завршавају са `.conf`) у радном фолдеру.

```
# /etc/ipsec.conf - Openswan IPsec configuration file
#
# Manual:     ipsec.conf.5
#
# Please place your own config files in /etc/ipsec.d/ ending in .conf

version 2.0     # conforms to second version of ipsec.conf specification

# basic configuration
config setup
        # Debug-logging controls:  "none" for (almost) none, "all" for lots.
        # klipsdebug=none
        # plutodebug="control parsing"
        # For Red Hat Enterprise Linux and Fedora, leave protostack=netkey
        protostack=netkey
        nat_traversal=yes
        #virtual_private=
        oe=off
        interfaces=%defaultroute
        # Enable this if you see "failed to find any available worker"
        # nhelpers=0

#You may put your configuration (.conf) file in the "/etc/ipsec.d/" and
uncomment this.
include /etc/ipsec.d/*.conf
```

2. Како би се подаци за аутентификацију различитих тунела поставили у различите фајлове (који морају да се завршавају са `.secrets`) у радном фолдеру `/etc/ipsec.d/`, потребно је да у `/etc/ipsec.secret` фајл упишите следећу линију (обавезно фајл завршити празним редом):

```
include /etc/ipsec.d/*.secrets
```

За аутентификацију RADIUS сервера институције и иAMPEC сервера, између којих се успоставља IPsec тунел, користе се X.509 дигитални сертификати. У ту сврху могу се користити TERENA сертификати или било који други сертификати који морају бити потписани неким CA сертификатом. На страни иAMPEC сервера користиће се TERENA дигитални сертификат.

3. Постављање CA сертификата

   i. У `/etc/ipsec.d` директоријуму потребно је да креирате `cacerts` директоријум уколико већ не постоји:

```
$ mkdir /etc/ipsec.d/cacerts
```

   ii. У `cacerts` директоријуму потребно је да поставите AddTrust_External_CA_Root, TERENA_SSL_CA, UTN-USERFirst-Hardware сертификате (то су сертификати из ланца поверења ком припада сертификат иAMPEC сервера):

```
$ wget http://www.amres.ac.rs/images/stories/servisi/TERENA_SSL_CA.pem
$ wget http://www.amres.ac.rs/images/stories/servisi/UTN-USERFirst-Hardware.pem
$ wget http://www.amres.ac.rs/images/stories/servisi/AddTrust_External_CA_Root.pem
$ wget http://www.amres.ac.rs/images/stories/servisi/TERENA_SSL_CA_2.pem
$ wget
http://www.amres.ac.rs/images/stories/servisi/USERTrust_RSA_Certification_Authority.pem
```

НАПОМЕНА: Уколико институција не користи TERENA сертификате потребно је да CA сертификате и све прелазне сертификате из ланца поверења ком припада сертификат RADIUS сервера институције, пошаљете AMPEC администритатору.

4. Подешавање сертификата RADIUS сервера институције

Потребно је да импортујете сертификат и приватни кључ RADIUS сервера институције у `nss` базу коју `openswan/libreswan` користи за читање сертификата.

   i. Уколико `nss` база није креирана (у `/etc/ipsec.d` фолдеру не постоји `cert8.db`), креирајте је на следећи начин:

      a. покрените `modutil` команду:

```
$ modutil -fips false -dbdir /etc/ipsec.d
```

      b. притисните ентер

      c. креирајте `nss` базу:

```
$ certutil -N -d /etc/ipsec.d
```

      d. притисните ентер два пута.

ii. Када је `nss` база креирана, потребно да генеришете PKCS#12 формат сертификата који садржи све потребне информације. Опција `-name` омогућава да дефинишете име под којим ће сертификат бити импортован у `nss` базу.

```
$ openssl pkcs12 -export -in /etc/pki/tls/certs/radius.pem -inkey
/etc/pki/tls/private/radius.key -name RADIUS-INST -out
/etc/pki/tls/certs/radius.p12
```

НАПОМЕНА: У упутству се подразумева да се сертификат сервера налази у `/etc/pki/tls/` директоријуму.

iii. Притисните ентер за креирање PKCS#12 сертификата без лозинке.

iv. Креирани PKCS#12 сертификат импортујте у `nss` базу следећом командом:

```
$ pk12util -i /etc/pki/tls/certs/radius.p12 -d /etc/ipsec.d
```

v. Притисните ентер.

vi. Да би проверили да ли је сертификат исправно импортован у `nss` базу искористите следећу команду:

```
$ certutil -L -d /etc/ipsec.d/
Certificate Nickname                                         Trust Attributes

SSL,S/MIME,JAR/XPI


RADIUS-INST                                                  u,u,u
```

vii. У `/etc/ipsec.d/` директоријуму креирајте фајл `radius-isnt.certs` и упишите име под којим је сертификат RADIUS сервера институције импортован у `nss` базу (обавезно фајл завршити празним редом):

```
$ touch radius-inst.secrets
: RSA "RADIUS-INST" ""

```

5. Креирајте конфигурацион фајл

```
$ touch iamres.conf
conn iamres
        # opsta podesavanja
        type=tunnel
        keyexchange=ike
        pfs=yes
        authby=rsasig
        # RADIUS server
        left=147.91.x.y #ip adresa radius servera institucije
        leftid=@radius.inst.bg.ac.rs # dns ime radius servera institucije
        leftrsasigkey=%cert #za autentifikaciju se koriste x.509 sertfikati
```

```
        leftcert=RADIUS-INST #ime sertifikata u nss bazi
        # iAMRES server
        right=147.91.1.11
        rightid=@login.iamres.amres.ac.rs
        rightrsasigkey=%cert
        rekey=no
        auto=start
```

НАПОМЕНА: Конфигурациони фајл копирајте без коментара и без празних редова. Обавезно фајл завршите празним редом (кликнути ентер након последњег реда).

6. Покрените IPsec:

```
$ service ipsec start
```

7. Иницирајте креирање IPsec тунела (позива се име конекције из конфигурационог фајла):

```
$ ipsec auto --up iamres
```

8. За проверу статуса IPsec тунела користите команду:

```
$ ipsec auto --status
```

9. Да би проверили да ли кроз тунел пролази саобраћај између RADIUS сервера институције и иAMPEC сервера, можете користити `tcpdump`. Предлози за команде које се могу користи су:

```
$ tcpdump -ni eth0 -X -v proto ESP
```

или

```
$ tcpdump -n -i eth0 esp or udp port 500 or udp port 4500
```

НАПОМЕНА: Логови од значаја се налазе у `/var/log/secure` фајлу.

4 Подешавање IPsec тунела на Debian и UBUNTU оперативним системима

4.1 Инсталација IPsec пакета

1. За реализацију IPsec тунела између RADIUS сервера институције и иAMPEC сервера потребно је да на RADIUS серверу институције инсталирате openswan, which и lsof пакете.

```
$ apt-get install openswan which lsof
```

Приликом инсталације појавиће се прозор са питањем да ли ће openswan користити X.509 сертификате на хосту. Потребно је да одаберете опцију **YES**. Након тога одаберите да ће сертификати бити импортовани (опција **import**). Остале кораке можете да прескочите (притиском на Enter).

2. Уколико није искључен, потребно је да искључите SELINUX

```
$ cat /etc/sysconfig/selinux
```

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - SELinux is fully disabled.
SELINUX=disabled
# SELINUXTYPE= type of policy in use. Possible values are:
#       targeted - Only targeted network daemons are protected.
#       strict - Full SELinux protection.
SELINUXTYPE=targeted

# SETLOCALDEFS= Check local definition changes
SETLOCALDEFS=0
```

3. Након инсталације је потребно да унесете промене у `/etc/susctl.conf` фајл на следећи начин (обратити пажњу да је неким променљивим потребно променити вредност, а неке је потребно додати):

```
# IPSec
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.eth0.rp_filter = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.ipv4.conf.default.log_martians = 0
net.ipv4.ip_forward = 1
```

4. Након ових промена потребно је поново да покренете sysctl следећом командом:

```
$ sysctl -p
```

5. Када су инсталирани сви неопходни алати могуће је покренути Ipsec сервис и тестирати инсталацију, односно тестирати да ли је сервис покенут како треба.

```
$ service ipsec start
$ ipsec verify
```

i. Излаз команде ipsec verify, када је све покренуто како треба, треба да изгледа овако:

```
Checking your system to see if IPsec got installed and started correctly:
Version check and ipsec on-path                                 [OK]
Linux Openswan U2.6.37/K3.2.0-23-generic (netkey)
Checking for IPsec support in kernel                            [OK]
 SAref kernel support                                           [N/A]
 NETKEY:  Testing XFRM related proc values                      [OK]
```

```
        [OK]
        [OK]
Checking that pluto is running                                  [OK]
 Pluto listening for IKE on udp 500                             [OK]
 Pluto listening for NAT-T on udp 4500                          [OK]
Checking for 'ip' command                                       [OK]
Checking /bin/sh is not /bin/dash                               [WARNING]
Checking for 'iptables' command                                 [OK]
Opportunistic Encryption Support                                [DISABLED]
```

6. За RADIUS сервер институције потребно је да отворите следеће портове:
   - UDP port 500 за Internet Key Exchange (IKE) протокол
   - UDP port 4500 за IKE NAT-Traversal
   - Protocol 50 за Encapsulated Security Payload (ESP) IPsec пакете

4.2 Конфигурација IPsec тунела

Радни фолдер openswan пакета инсталираног на начин описан у поглављу 4.1 је /etc/ipsec.d

Фајлови од значаја су `/etc/ipsec.conf`, главни конфигурациони фајл, и `/etc/ipsec.secret`, фајл који се користи у процесу аутентификације сервера између којих се успоставља IPsec тунел. У зависности од начина аутентификације, у фајл `ipsec.secret` је потребно да поставите дељене кључеве, RSA потписе или показиваче на X.509 дигиталне сертификате.

Више информација о овим фајловима можете добити на страницам упутства за коришћење команди `ipsec.conf` и `ipsec.secrets` (коришћењем `man` команде).

1. У главном конфигурационом фајлу, `/etc/ipsec.conf`, потребно је да вредност променљиве `protostack` подесити да буде `netkey`. Такође је потребно да уклоните коментар у последњој линији, испред `include /etc/ipsec.d/*.conf`, како би се конфигурације конкретних IPsec тунела раздвојиле у посебне конфигурационе фајлове (који морају да се завршавају са .conf) у радном фолдеру.

```
# /etc/ipsec.conf - Openswan IPsec configuration file

# This file:  /usr/share/doc/openswan/ipsec.conf-sample
#
# Manual:     ipsec.conf.5


version 2.0     # conforms to second version of ipsec.conf specification

# basic configuration
config setup
        # Do not set debug options to debug configuration issues!
        # plutodebug / klipsdebug = "all", "none" or a combation from below:
        # "raw crypt parsing emitting control klips pfkey natt x509 dpd
private"
        # eg:
        # plutodebug="control parsing"
        # Again: only enable plutodebug or klipsdebug when asked by a
developer
        #
        # enable to get logs per-peer
        # plutoopts="--perpeerlog"
        #
        # Enable core dumps (might require system changes, like ulimit -C)
        # This is required for abrtd to work properly
        # Note: incorrect SElinux policies might prevent pluto writing the
core
        dumpdir=/var/run/pluto/
```

```
        #
        # NAT-TRAVERSAL support, see README.NAT-Traversal
        nat_traversal=yes
        # exclude networks used on server side by adding %v4:!a.b.c.0/24
        # It seems that T-Mobile in the US and Rogers/Fido in Canada are
        # using 25/8 as "private" address space on their 3G network.
        # This range has not been announced via BGP (at least upto 2010-12-
21)

virtual_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.16.0.0/12,%v4:25.0.
0.0/8,%v6:fd00::/8,%v6:fe80::/10
        # OE is now off by default. Uncomment and change to on, to enable.
        oe=off
        # which IPsec stack to use. auto will try netkey, then klips then
mast
        protostack=netkey
        # Use this to log to a file, or disable logging on embedded systems
(like openwrt)
        #plutostderrlog=/dev/null
# Add connections here

# sample VPN connection
# for more examples, see /etc/ipsec.d/examples/
#conn sample
#               # Left security gateway, subnet behind it, nexthop toward
#               left=10.0.0.1
#               leftsubnet=172.16.0.0/24
#               leftnexthop=10.22.33.44
#               # Right security gateway, subnet behind it, nexthop toward #
right=10.12.12.1
#               rightsubnet=192.168.0.0/24
#               rightnexthop=10.101.102.103
#               # To authorize this connection, but not actually start it,
#               # at startup, uncomment this.
#               #auto=add
include /etc/ipsec.d/*.conf
```

НАПОМЕНА: Уколико оваква линија не постоји, додајте је на крају `ipsec.conf` конфигурационог фајла и обавезно фајл завршите празним редом (кликнути Ентер након последњег реда).

2. Како би се подаци за аутентификацију различитих тунела поставили у различите фајлове (који морају да се завршавају са `.secrets`) у радном фолдеру `/etc/ipsec.d/`, потребно је да у `/etc/ipsec.secret` фајл упишите следећу линију (обавезно фајл завршити празним редом):

```
include /etc/ipsec.d/*.secrets
```

За аутентификацију RADIUS сервера институције и иAMPEC сервера, између којих се успоставља IPsec тунел, треба да се користе X.509 дигитални сертификати. У ту сврху можете да користите TERENA сертификате или било које друге сертификате који морају бити потписани неким CA сертификатом. На страни иAMPEC сервера користиће се TERENA дигитални сертификат.

3. Постављање CA сертификата

   У `/etc/ipsec.d/` налазе се три директоријума од важности: `cacert`, `certs` и `private`.

   i. У `/etc/ipsec.d/cacerts` директоријуму је потребно да поставите AddTrust_External_CA_Root, TERENA_SSL_CA, UTN-USERFirst-Hardware сертификате (то су сертификати из ланца поверења ком припада сертификат iAMRES сервера).

```
$ wget http://www.amres.ac.rs/images/stories/servisi/TERENA_SSL_CA.pem
$ wget http://www.amres.ac.rs/images/stories/servisi/UTN-USERFirst-Hardware.pem
$ wget http://www.amres.ac.rs/images/stories/servisi/AddTrust_External_CA_Root.pem
$ wget http://www.amres.ac.rs/images/stories/servisi/TERENA_SSL_CA_2.pem
$ wget
http://www.amres.ac.rs/images/stories/servisi/USERTrust_RSA_Certification_Authority.pem
```

НАПОМЕНА: Уколико институција не користи TERENA сертификате потребно је да CA сертификате и све прелазне сертификате из ланца поверења ком припада сертификат RADIUS сервера институције, пошаљете AMPEC администритатору.

4. Подешавање сертификата RADIUS сервера институције

   i. Потребно је да копирате сертификат RADIUS сервера институције у `/etc/ipsec.d/certs` директоријум.

```
$ cp /etc/pki/tls/certs/radius.pem /etc/ipsec.d/certs/radius.pem
```

НАПОМЕНА: У упутству се претпоставља да се сертификат сервера налази у `/etc/pki/tls/certs` директоријуму.

   ii. Потребно је да копирате приватни кључ RADIUS сервера институције у `/etc/ipsec.d/private` директоријум.

```
$ cp /etc/pki/tls/private/radius.key /etc/ipsec.d/private/radius.key
```

НАПОМЕНА: У упутству се претпоставља да се приватни кључ сервера налази у `/etc/pki/tls/private/` директоријуму.

   iii. Креирајте фајл `radius-inst.secrets` у `/etc/ipsec.d/` директоријуму и упишите директоријум у ком се налази приватни кључ RADIUS сервера институције (обавезно фајл завршити празним редом):

```
$ touch radius-inst.secrets
: RSA /etc/ipsec.d/private/radius.key ""
```

5. Креирајте конфигурацион фајл

```
$ touch iamres.conf
conn iamres
        # opsta podesavanja
        type=tunnel
        keyexchange=ike
        pfs=yes
        authby=rsasig
        # RADIUS server
        left=147.91.x.y #ip adresa radius servera institucije
        leftid=@radius.inst.bg.ac.rs # dns ime radius servera institucije
        leftrsasigkey=%cert
        leftcert=/etc/ipsec.d/certs/radius.pem #lokacija sertifikata
        right=147.91.1.11
        rightid=@login.iamres.amres.ac.rs
        rightrsasigkey=%cert
        rekey=no
        auto=start
```

НАПОМЕНА: Конфигурациони фајл копирајте без коментара и без празних редова. Обавезно фајл завршите празним редом (кликнути Ентер након последњег реда).

6. Покрените IPsec :

```
$ service ipsec start
```

7. Иницирајте креирање IPsec тунела (позива се име конекције из конфигурационог фајла):

```
$ ipsec auto --up iamres
```

8. За проверу статуса IPsec тунела користите команду:

```
$ ipsec auto --status
```

9. Да би проверили да ли кроз тунел пролази саобраћај између RADIUS сервера институције и iAMRES сервера, можете да користите `tcpdump`. Предлози за команде које се могу користи су:

```
$ tcpdump -ni eth0 -X -v proto 50
```

или

```
$ tcpdump -n -i eth0 esp or udp port 500 or udp port 4500
```

НАПОМЕНА: Логови од значаја се налазе у `/var/log/auth.log` фајлу.