

Konfiguracja serwerów regionalnych

- etap 2, wdrożenie protokołu RadSec

Maja Górecka-Wolniewicz, UCI UMK (mgw@umk.pl)
dokument przygotowany w ramach projektu B-R eduroam-PIONIER
wersja 1.0

Spis treści

1. Wstęp.....	1
2. Przygotowanie kluczy.....	1
3. Przykład konfiguracji.....	2
3.1. Plik /etc/radsecproxy.conf	2
3.2. Plik /etc/radsecproxy.conf.d/clients.conf	2
3.3. Plik /etc/radsecproxy.conf.d/servers.conf.....	2
3.4. Plik /etc/radsecproxy.conf.d/realms.conf.....	3

1. Wstęp

W pierwszym etapie wdrażania usługi eduroam serwery regionalne używały do komunikacji modelu hierarchicznego oraz protokołu RADIUS opartego na UDP. Opis podstawowej konfiguracji serwera radsecproxy został przedstawiony w dokumencie [1]. W drugim etapie pozostajemy przy hierarchicznej strukturze serwerów, ale komunikacja między serwerami ma się odbywać zgodnie z protokołem RadSec opartym na transporcie TLS, realizowanym w bezpiecznym tunelu TLS ([3], [4]).

W tym celu każdy serwer regionalny musi mieć odpowiedni certyfikat. Zgodnie z opisem [2], serwery regionalne będą docelowo wpięte w dynamiczną strukturę europejską. Każdy administrator serwera regionalnego otrzyma od Koordynatora, za pomocą bezpiecznej formy komunikacji, pliki certyfikatów, które należy wskazać w konfiguracji w bloku tls. Europejski urząd certyfikacyjny przeznaczony dla środowiska usług akademickich, takich jak np. eduroam, działa obecnie w wersji pilotowej, dlatego pozyskiwanie certyfikatów na tym etapie musi być realizowane za pośrednictwem Koordynatora eduroam w Polsce.

Wszystkie bezpieczne połączenia będą korzystały z certyfikatu serwera, natomiast do weryfikacji certyfikatów będzie używany wskazany certyfikat urzędu CA. W przypadku usługi eduroam certyfikaty serwera są podpisane przez urząd eduGAINSCA, podlegający pod eduGAINCA (<http://sca.edugain.org/cacert/>).

Docelowo w polskiej usłudze eduroam zostanie wdrożony dynamiczny RadSec, korzystający z usługi DNS do pozyskania informacji o serwerze obsługującym daną domeną (realm).

2. Przygotowanie kluczy

Administrator serwera regionalnego otrzymuje od koordynatora:

- plik zawierający klucz serwera w postaci PKCS12 (rozszerzenie .p12);
- hasło importu klucza PKCS12;
- plik zawierający certyfikaty nadrzędne: eduGAIN-chain.pem.

Klucz w postaci PKCS12 należy przekształcić do pary certyfikat w postaci PEM oraz klucz prywatny serwera za pomocą następujących poleceń, podając otrzymane hasło importu:

```
openssl pkcs12 -in radius.p12 -clcerts -nokeys -out radius.pem
```

W pliku radius.pem powstanie certyfikat serwera w postaci PEM.

```
openssl pkcs12 -in radius.p12 -nocerts -out radius.key
```

W pliku radius.key powstanie klucz prywatny serwera.

3. Przykład konfiguracji

3.1. Plik /etc/radsecproxy.conf

Definiujemy sekcję tls o postaci:

```
# definiujemy pliki certyfikatu serwera, klucza prywatnego oraz CA
tls default {
CACertificateFile    /etc/radsecproxy.conf.d/eduGAIN-chain.pem
CertificateFile      /etc/radsecproxy.conf.d/radius.pem
CertificateKeyFile   /etc/radsecproxy.conf.d/radius.key
# jeśli klucz prywatny nie jest zaszyfrowany,
# kasujemy opcję CertificateKeyPassword
CertificateKeyPassword "aaaa"
}
```

3.2. Plik /etc/radsecproxy.conf.d/clients.conf

Definiujemy klientów, którzy mogą kontaktować się z serwerem regionalnym poprzez protokół TLS.

Zezwalamy na komunikację tego typu z serwerami krajowymi.

```
Client PL1TLS {
type tls
host radius1.eduroam.pl
matchCertificateAttribute
SubjectAltName:URI:/^https:\\/\\/registry.edugain.org\\/resolver\\?
urn=urn:geant:eduroam:component:proxy:Europe:PIONIER:PL$/
}
Client PL2TLS {
type tls
host radius2.eduroam.pl
matchCertificateAttribute
SubjectAltName:URI:/^https:\\/\\/registry.edugain.org\\/resolver\\?
urn=urn:geant:eduroam:component:proxy:Europe:PIONIER:PL$/
}
```

Dyrektywa matchCertificateAttribute ustala zasadę dopasowywania certyfikatu partnera na podstawie zawartości rozszerzenia Subject Alternative Name. Napis zawierający w parametrze urn wartość

urn:geant:eduroam:component:proxy:Europe:PIONIER:PL
jest specyficzny dla serwerów poziomu krajowego.

Uwaga! matchCertificateAttribute i dwa kolejne wiersze należy umieścić jednym wierszem, przed SubjectAltName musi znajdować się spacja.

Dyrektywy konfigurujące klientów PL1TLS i PL2TLS zostały umieszczone w pliku:

https://www.eduroam.pl/Dokumentacja/radsecproxy_conf.tar.gz

Jeśli chcemy wyłączyć domyślne sprawdzenie zgodności nazwy domenowej klienta z nazwą umieszczoną w CN lub SubjectAltName, to należy dodać w bloku Client:

```
certificateNameCheck off
```

3.3. Plik /etc/radsecproxy.conf.d/servers.conf

Definiujemy serwery, z którymi chcemy kontaktować się poprzez TLS. Na tym etapie wdrażania usługi chcemy zagwarantować bezpieczną komunikację z serwerami krajowymi, definiujemy więc:

```
Server PL1TLS {
type tls
host radius1.eduroam.pl
matchCertificateAttribute
SubjectAltName:URI:/^https:\\/\\/registry.edugain.org\\/resolver\?
urn=urn:geant:eduroam:component:proxy:Europe:PIONIER:PL$/
}
Server PL2TLS {
type tls
host radius2.eduroam.pl
matchCertificateAttribute
SubjectAltName:URI:/^https:\\/\\/registry.edugain.org\\/resolver\?
urn=urn:geant:eduroam:component:proxy:Europe:PIONIER:PL$/
}
```

Uwaga! matchCertificateAttribute i dwa kolejne wiersze należy umieścić jednym wierszem, przed SubjectAltName musi znajdować się spacja.

Dyrektywy konfigurujące serwery PL1TLS i PL2TLS zostały umieszczone w pliku:

https://www.eduroam.pl/Dokumentacja/radsecproxy_conf.tar.gz

Jeśli chcemy wyłączyć domyślne sprawdzenie zgodności nazwy domenowej serwera z nazwą umieszczoną w CN lub SubjectAltName, to należy dodać w bloku Client:

```
certificateNameCheck off
```

3.4. Plik /etc/radsecproxy.conf.d/realms.conf

W pliku /etc/radsecproxy.conf.d/realms.conf wskazujemy, że obsługa domyślnej domeny (*) jest realizowana poprzez serwery PL1TLS i PL2TLS.

3.5. Dostęp do portu RadSec

Port 2083, domyślny port RadSec musi być otwarty dla serwerów krajowych.

Materiały towarzyszące

- [1] *Konfiguracja serwerów regionalnych*, dokument przygotowany w ramach projektu B-R eduroam-PIONIER
- [2] *Koncepcja wdrożenia usługi eduroam w sieci Pionier*, dokument przygotowany w ramach projektu B-R eduroam-PIONIER
- [3] *RadSec, a secure, reliable RADIUS Protocol*, Open System Consultants Pty. Ltd., <http://www.open.com.au/radiator/radsec-whitepaper.pdf>

[4] *RadSec Version 2 - A Secure and Reliable Transport for the RADIUS Protocol*, draft-winter-radsec-1, <http://tools.ietf.org/html/draft-winter-radsec-01>