Projekt nr. POIG.02 03. 00-00-028/08-01
www.platon.pionier.net.pl
PLATFORMA OBSŁUGI NAUKI PLATON
KOORDYNATOR: INSTYTUT CHEMII BIOORGANICZNEJ PAN
POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE
ul. Noskowskiego 12/14, 61-704 Poznań, (+48 61) 858 20 00, fax: (+48 61) 852 59 54, e-mail: office@man.poznan.pl, www: http://www.man.poznan.pl

Zasady obsługi incydentów sieciowych w usłudze eduroam

Maja Górecka-Wolniewicz, UCI UMK (mgw@umk.pl)
Zbigniew Ołtuszyk, PCSS (zbigniew.oltuszyk@man.poznan.pl)
Tomasz Wolniewicz, UCI UMK (twoln@umk.pl)
dokument przygotowany w ramach projektu B-R eduroam-PIONIER
Zaktualizowany w ramach projektu PLATON
wersja 2.0 – lipiec 2012

Spis treści

1. Wstęp

Zgodnie z definicją europejskiej usługi eduroam [1] oraz z dokumentem *Koncepcja wdrożenia usługi eduroam w sieci PIONIER* [3], usługa ta opiera się w znacznym stopniu na wzajemnym zaufaniu instytucji współuczestniczących jej budowaniu. Kluczowym ogniwem zaufania jest gwarancja, że każda nieprawidłowość w zakresie funkcjonowania usługi zostanie szybko wyjaśniona. Dodatkowo, obsłużone incydenty sieciowe mają poprawiać ogólne bezpieczeństwo, dlatego duży nacisk kładzie się na współpracę ośrodków korzystających z usługi i na propagowanie zdobytych doświadczeń.

W niniejszym dokumencie opisujemy sposób reakcji na incydenty sieciowe. Podstawowym wymogiem działania przedstawionych procedur jest przechowywanie przez wszystkie jednostki uczestniczące w usłudze eduroam zapisów dotyczących uwierzytelniania oraz przypisywania adresów IP klientom eduroam.

Administratorzy eduroam muszą pamiętać, że funkcjonowanie mechanizmów udostępniania sieci bezprzewodowej w ich instytucji wpływa znacząco na obraz ogólnoeuropejskiej usługi eduroam. Dlatego, aby usługa działała zgodnie z zaprojektowanym modelem, wszędzie muszą być stosowane zalecane zabezpieczenia.

2. Incydent sieciowy

2.1. Definicja

Incydentem sieciowym nazywamy zdarzenie w sieci, które nastąpiło w określonym czasie i wiązało się z dostępem do zasobów sieciowych przez klienta o konkretnym adresie IP. Zazwyczaj takie zdarzenie polega na niewłaściwym korzystaniu z sieci, np. naruszeniu jej regulaminu, rozsyłaniu spamów, rozpowszechnianiu poprzez sieć materiałów chronionych prawem autorskim, skanowaniu hostów w Internecie, próbach włamań itp. Często o incydencie sieciowym dowiadujemy się z powodu skargi innych użytkowników sieci, albo przez zgłoszenie nadużyć pochodzące z innych instytucji lub od właścicieli chronionych zasobów.

2.2. Obsługa

Incydent sieciowy dotyczy eduroam, jeśli wiąże się z pulą adresów IP wykorzystywanych w eduroam. Wyjaśnienie incydentu sieciowego polega na powiązaniu zdarzenia z konkretnym użytkownikiem, a następnie w zależności od oceny stopnia stworzonego zagrożenia, pouczeniu użytkownika, lub zablokowaniu możliwości korzystania z usługi eduroam przez danego użytkownika lub przez wszystkich użytkowników danej domeny. Incydent związany ze złamaniem prawa może mieć konsekwencje w postaci dochodzenia prowadzonego przez organy ścigania i to do nich należy podjęcie odpowiednich kroków formalnych. Obsługa incydentu musi uwzględniać ograniczenia nakładane przez przepisy ochrony danych osobowych.

2.2.1. Adres sieciowy i fizyczny klienta eduroam

Punktem wyjścia jest źródłowy adres IP incydentu. Na jego podstawie powinno być możliwe ustalenie przebiegu zdarzenia, a np. w oparciu o logi serwera DHCP, adresu fizycznego (MAC) klienta. Aby pierwsza faza obsługi incydentu funkcjonowała poprawnie, zalecane jest zapewnienie przez dostawcę eduroam w instytucji, by:

1. adres IP jednoznacznie identyfikował użytkownika w danym czasie – w tym celu polski regulamin *eduroam* ([2]), w ślad za europejskim, sugeruje, by instytucja udostępniająca sieć poprzez eduroam nie stosowała technologii NAT, która zdecydowanie utrudnia właściwą obsługę incydentów sieciowych – dostawca nie jest wówczas w stanie powiązać zdarzenia z konkretnym użytkownikiem;
2. klient eduroam nie miał możliwości, po otrzymaniu dostępu do sieci, zmiany adresu IP i kontynuowania pracy w sieci z obcym adresem.

Pierwsze zalecenie jest stosunkowo łatwe w realizacji, trzeba jedynie dysponować odpowiednimi zapasami adresów sieciowych. Serwer DHCP odpowiedzialny za przydzielanie adresów internetowych korzysta wówczas ze wskazanej puli adresów publicznych.

Drugie zalecenie wymaga nieco większego wkładu pracy. Należy zagwarantować, by uprawnienia do korzystania z sieci wiązały się z parą (adres IP, MAC), a nie wyłącznie z adresem fizycznym. W tym celu należy domyślnie wyłączyć prawo korzystania z sieci, a w chwili przydzielania adresowego przez serwer DHCP otwierać dostęp sieciowy dla konkretnej pary IP i MAC.

Jeśli użytkownik samodzielnie zmieni swój adres sieciowy na statyczny, to utraci dostęp do sieci. Gdyby nie był zaimplementowany powyżej opisany mechanizm, klient mógłby po takiej zmianie kontynuować pracę w sieci z nadanym sobie samodzielnie adresem IP. W takiej sytuacji w przypadku incydentu sieciowego administrator nie byłby w stanie wskazać winnego, lub wina spadłaby na niewłaściwego użytkownika.

2.2.2. Sesja uwierzytelnienia

Gdy są już znane adresy IP i MAC klienta, kolejną fazą identyfikacji incydentu jest powiązanie tych danych z konkretną sesją uwierzytelnienia. W tym celu należy znaleźć właściwą sesję uwierzytelniania na podstawie daty i czasu zdarzenia oraz adresu MAC. Z lokalnej konfiguracji eduroam wynika, na jakim serwerze mogło nastąpić uwierzytelnienie. Efektem tej fazy analizy incydentu jest identyfikator związany z uwierzytelnieniem konkretnego użytkownika. Należy tu wyróżnić dwie możliwe sytuacje dotyczące znalezionej sesji uwierzytelnienia:

1. sesja wskazuje użytkownika lokalnego i w logach serwera widzimy pełny zapis sesji uwierzytelnienia – identyfikator dotyczy domeny obsługiwanej przez serwer RADIUS danej instytucji;
2. sesja dotyczy użytkownika zewnętrznego – identyfikator zawiera domenę nie obsługiwaną lokalnie.

Gdy źródłem incydentu sieciowego jest użytkownik lokalny, to nie mamy do czynienia z naruszeniem dotyczącym gościnnego dostępu do usługi eduroam i dalsze postępowanie jest podobne, jak w przypadku każdego innego nadużycia związanego z lokalną siecią. Istnieje wówczas możliwość samodzielnej, szczegółowej dalszej analizy źródła incydentu, gdyż znamy lokalne metody uwierzytelniania i potrafimy powiązać identyfikator uwierzytelnienia z konkretną osobą. O tym, że naruszenie zasad korzystania z sieci wiąże się z aktywnością użytkownika lokalnego możne już świadczyć sam numer IP zdarzenia – jest tak, gdy użytkownicy eduroam są umieszczani w odpowiednich VLAN-ach.

W drugim przypadku możemy jedynie stwierdzić, że użytkownik posługujący się danym identyfikatorem uzyskał dostęp do sieci dzięki usłudze eduroam. W dalsze dochodzenie w sprawie incydentu sieciowego musi zostać włączony administrator serwera uwierzytelniania w domenie występującej w identyfikatorze.

2.2.3. Przekazanie zgłoszenia do dalszej obsługi

Jeśli analizowany incydent, dotyczący usługi eduroam, wiąże się z użytkownikiem z domeny zewnętrznej, należy przekazać informację o zdarzeniu:

- swojemu operatorowi regionalnemu, gdy dotyczy domeny polskiej,
- Koordynatorowi eduroam w Polsce, gdy dotyczy domeny zagranicznej.

Operator regionalny, w przypadku, gdy incydent wiąże się z domeną przekierowywaną na serwerze regionalnym do serwera instytucji podległej danemu operatorowi, dostarcza dane zdarzenia do administratora właściwej instytucji. W przeciwnym razie informacje o incydencie otrzymuje Koordynator eduroam w Polsce.

Koordynator przekazuje dane związane z incydentem do właściwego administratora w instytucji, lub w przypadku incydentów zagranicznych, uruchamia kanały europejskiej usługi eduroam.

Administrator eduroam w macierzystej jednostce lokalizuje sesję uwierzytelnienia danego użytkownika, na podstawie otrzymanych danych: daty i godziny, adresu MAC oraz identyfikatora uwierzytelnienia.

Jeżeli incydent dotyczy złamania regulaminu lokalnego, etykiety sieciowej lub innego wykroczenia nie powodującego rozpoczęcia dochodzenia przez organy ścigania, to jednostka macierzysta powinna podjąć stosowne działania, tak by zapobiec powtórzeniu się tego typu sytuacji. Nagminne powodowanie incydentów przez osoby związane z daną instytucją może doprowadzić do zablokowania możliwości korzystania z usługi eduroam przez całą instytucję. Nie oczekuje się, aby administrator jednostki macierzystej udostępniał jakiekolwiek dane osobowe użytkownika. Stanowiłoby to naruszenie prawa. Doświadczenie pokazuje, że samo pouczenie użytkownika jest całkowicie wystarczające.

Incydenty o zasięgu międzynarodowym powinny być zgłaszane krajowym CERT-om.

W przypadku poważnych incydentów, w sprawie których prowadzone jest dochodzenie, inicjatywę należy pozostawić właściwym organom ścigania, przekazując im stosowne informacje i opis procedur usługi eduroam. Operatorzy regionalni oraz Koordynator usługi eduroam w Polsce będą wspomagać instytucję w wyjaśnieniu sprawy.

Kontakt z operatorem regionalnym, Koordynatorem eduroam oraz administratorem eduroam w instytucji powinien odbywać się w sposób bezpieczny, zaleca się wsparcie komunikacji poprzez pocztę elektroniczną technologiami PGP lub S/MIME.

Instytucja, na której terenie doszło do incydentu ma prawo tak zmodyfikować konfigurację usługi eduroam na swoim terenie, by dany użytkownik, lub wszyscy użytkownicy w danej domenie (jeśli nie jest możliwa jednoznaczna identyfikacja użytkownika, patrz p. 4) nie mieli dostępu do usługi do czasu wyjaśnienia problemu.

3. Przechowywanie informacji dotyczącej usługi eduroam

Zgodnie z polskim regulaminem *eduroam* zapisy dotyczące korzystania z usługi eduroam muszą być przechowywane przez co najmniej sześć miesięcy.

Logi dotyczące dostępu gościnnego, w pierwszym rzędzie zabezpieczają instytucję udzielającą takiego dostępu. Gdyby pojawiło się zgłoszenie dotyczące jakiegoś incydentu, instytucja udzielająca dostępu będzie mogła skorzystać z logów, by przenieść odpowiedzialność na właściwego użytkownika.

Logi dostępu gościnnego są jednak istotne również dla usługi eduroam jako całości. Stosunkowo typowym zachowaniem użytkowników jest zgłaszanie problemów z dostępem gościnnym dopiero po powrocie do instytucji macierzystej. W takich sytuacjach warto jest wyjaśnić problem, aby zapobiec wystąpieniu go w przyszłości i poprawić działanie usługi eduroam jako całości. Posiadanie logów dostępu gościnnego będzie w takiej sytuacji niezbędne.

Aby była możliwa analiza incydentów sieciowych, według procedury opisanej w części 2, niezbędne jest przechowywanie zarówno danych dotyczących przydzielania adresu IP w eduroam (zadanie serwera DHCP), jak i realizacji sesji uwierzytelnienia (rola serwera RADIUS). Administrator usługi eduroam w instytucji powinien być przygotowany, by szybko zidentyfikować incydent, dlatego zaleca się zbudowanie odpowiedniej infrastruktury zapisu zdarzeń DHCP i uwierzytelniania RADIUS. Najlepiej, by oba źródła miały wspólne miejsce logowania, np. plik, czy bazę danych. W przypadku uwierzytelniania trzeba również wziąć pod uwagę, że zapisy mogą się pojawić na jednym ze zdefiniowanych serwerów – podstawowym lub zapasowym.

Należy zadbać o to, by zegary wszystkich serwerów i urządzeń biorących udział w tworzeniu logów były synchronizowane przy pomocy usługi NTP.

3.1. Logi DHCP

Zapisy w logach DHCP są niezbędne do analizy zgłoszonych incydentów. Dlatego należy zagwarantować, by po pierwsze w logach znalazły się informacje dotyczące przydzielenia adresu IP adresowi MAC, po drugie, by logi były archiwizowane przez zalecany czas sześciu miesięcy.

3.2. Zapisy uwierzytelniania serwera RADIUS

Każde udane uwierzytelnienie dokonane przez serwer RADIUS musi zostać odnotowane i przechowane przez sześć miesięcy, analogicznie jak w przypadku zapisów DHCP. Serwer instytucji, na którym jest realizowana obsługa uwierzytelniania w konkretnej domenie musi po udanej weryfikacji danych uwierzytelniania zapisać w logu informację dotyczącą uwierzytelnienia. Powinna ona zawierać: datę i czas, identyfikator użytkownika, adres fizyczny karty. Typowo serwer FreeRADIUS zapisuje również nazwę lub adres IP urządzenia sieciowego (Access Point, kontroler lub serwer pośredniczący), za pośrednictwem którego zostało przekazane zlecenie uwierzytelnienia. Zazwyczaj w instytucji działają dwa serwery, podstawowy i zapasowy – oba serwery muszą identycznie zapisywać informacje o uwierzytelnieniach. Należy rozważyć możliwość utrzymywania zapisów uwierzytelnień w relacyjnej bazie danych, w ten sposób dane będą dostępne w jednym miejscu, co ułatwi lokalizację potrzebnej informacji. W 5.3 opisujemy, jak można taką funkcjonalność zrealizować w oprogramowaniu FreeRADIUS.

3.3. Narzędzia wspomagające

Jeśli zostały wdrożone procedury opisane w 3.1. i 3.2, to dysponując pełną, łatwo dostępną informacją dotyczącą pracy DHCP oraz serwerów RADIUS w usłudze eduroam, można przygotować proste

skrypty operujące na tych danych. Będzie to duże udogodnienie pracy, nie tylko przy rozwikływaniu incydentów sieciowych, również przy zbieraniu statystyk.

4. Informacja o użytkowniku

Jeżeli mamy do czynienia z incydentem sieciowym, w którym uczestniczył użytkownik zewnętrzny, to po dokonaniu powiązania adres IP → adres MAC → identyfikator użytkownika, uzyskany napis użytkownik@domena najczęściej nie wskazuje jeszcze konkretnego użytkownika. Możemy mieć jedynie pewność, że chodzi o użytkownika w danej domenie. Nie oznacza to, że identyfikator logowania nie jest istotny dla administratora serwera tej domeny.

4.1. Tożsamość zewnętrzna i wewnętrzna *(inner and outer identity)*

Popularne metody uwierzytelnienia, z których korzysta większość instytucji uwierzytelniających, to PEAP i EAP-TTLS. Cechą wspólną tych metod jest przekazywanie właściwych danych uwierzytelniania w tunelu SSL, w zaszyfrowanym atrybucie `EAP-Message`. Dane te są przekazywane w typowym pakiecie RADIUS, zawierającym atrybut `User-Name`, na podstawie którego jest dedukowany sposób obsługi zlecenia. W tym przypadku atrybut `User-Name` przenosi nazwę tzw. tożsamości zewnętrznej użytkownika, często ma wartość `anonymous@domena`, lub `@domena`. Nazwa ta nie jest unikatową nazwą użytkownika. Unikatowy identyfikator użytkownika jest dostępny dopiero po rozszyfrowaniu komunikatu z atrybutu `EAP-Message`. Rozszyfrowanie jest realizowane na serwerze macierzystym użytkownika, więc tylko tam, w zapisach pracy serwera RADIUS, można znaleźć pełną informację dotyczącą uwierzytelnienia.

Dysponując informacją związaną wyłącznie z pośredniczeniem w realizacji zlecenia uwierzytelnienia, nie jesteśmy w stanie jednoznacznie wskazać użytkownika. Nawet jeśli identyfikator nie ma postaci `anonymous@domena`, czy `@domena`, lecz np. `stud1357@domena`, nie można traktować go jako wiążącego wskazania konkretnego użytkownika – za chwilę inny użytkownik może użyć takiego samego identyfikatora w polu zewnętrznej tożsamości, albo użytkownik, który spowodował problemy, będzie ubiegał się o dostęp do sieci wysyłając inną nazwę w polu `User-Name`. Należy zdawać sobie z tego sprawę, gdy reakcją na incydent jest chęć odcięcia dostępu do sieci poprzez odrzucanie zleceń zawierających określoną nazwę użytkownika.

4.2. Atrybuty `Operator-Name, User-Name` i `Chargeable-User-Identity`

4.2.1. Operator-Name

Atrybut Operator-Name jest zdefiniowany w RFC-5580 i służy przekazaniu informacji od operatora udzielanego dostępu do operatora macierzystego. W eduroam tego atrybutu używa się w celu poinformowania instytucji macierzystej o instytucji, w której użytkownik korzysta z usługi. Atrybut ten w eduroam jest również niezbędny do prawidłowej obsługi atrybutu Chargeable-User-Identity.

4.2.2. Identyfikacja użytkownika poprzez atrybut Chargeable-User-Identity

eduroam przykłada dużą wagę do zapewnienia maksymalnej ochrony prywatności użytkownika. W szczególności zaleca się, by w miarę możliwości nie ujawniać rzeczywistego identyfikatora użytkownika (zwłaszcza gdy identyfikator jest jednocześnie adresem mailowym użytkownika i stosunkowo łatwo może być z danym użytkownikiem powiązany). Najpopularniejsze metody EAP pozwalają na stosowanie odrębnego identyfikatora na potrzeby routingu pakietów (tzw. identyfikatora zewnętrznego) i odrębnego na potrzeby samego uwierzytelnienia. Instytucja udostępniająca sieć widzi wyłącznie identyfikator zewnętrzny, a on może być wspólny dla wszystkich użytkowników z jednej instytucji macierzystej. Oczywiście użytkownik może być zawsze zidentyfikowany na postawie logów instytucji udostępniającej sieć i instytucji macierzystej, taki proces wymaga jednak czasu i powinien być uruchamiany tylko przy obsłudze istotnych incydentów.

Stosowanie identyfikatorów zewnętrznych powoduje, że instytucja udostępniająca sieć nie może podejmować indywidualnych decyzji na podstawie wartości przekazanej w atrybucie User-Name. Jeżeli użytkownik narusza lokalny regulamin, to pierwszym krokiem może być zablokowanie kon-

kretnego adresu sprzętowego, ale jeżeli użytkownik działa z premedytacją, to adres sprzętowy może zmieniać. W takiej sytuacji jedynym działaniem nie wymagającym kontaktu z instytucją macierzystą, jest zablokowanie dostępu dla wszystkich użytkowników danej instytucji, poprzez blokadę całego realmu. Taka decyzja może jednak odciąć od sieci wielu użytkowników, więc powinna być podejmowana z rozwagą.

Znakomitym rozwiązaniem jest zastosowanie identyfikatora, który nie będzie zdradzał tożsamości użytkownika, ale jednocześnie będzie jednoznacznie go identyfikował. RFC-4372 [5] definiuje atrybut Chargeable-User-Identity, stworzony właśnie na takie potrzeby. Wartość atrybutu Chargeable-User-Identity jest generowana przez instytucję macierzystą na podstawie rzeczywistego identyfikatora użytkownika. eduroam idzie o krok dalej, wprowadzając mechanizmy umożliwiające analizę połączonych logów wielu instytucji w celu stwierdzenia, jakie instytucje były odwiedzane przez tego samego użytkownika. eduroam zakłada, że przy generowaniu Chargeable-User-Identity należy korzystać z wartości Operator-Name, tak by dla różnych wartości tego atrybutu generować różne wartości Chargeable-User-Identity.

Stosowanie Chargeable-User-Identity jest obecnie rekomendowane przez regulamin europejski oraz regulamin polski.

Jeśli chcemy wprowadzić funkcjonalność CUI musimy uwzględnić w konfiguracji serwera FreeRADIUS dwie rzeczy:

1. podczas uwierzytelniania serwer RADIUS musi zakładać, że atrybut CUI będzie wysyłany, dlatego należy na etapie sesji uwierzytelnienia wygenerować jego wartość, np. odczytać wartość lokalnego identyfikatora użytkownika podczas współpracy z bazą danych i utworzyć na jego podstawie wartość CUI;
2. po pozytywnym uwierzytelnieniu, należy sprawdzić, czy w zleceniu pojawił się atrybut CUI, jeśli tak, to w odpowiedzi jest umieszczana właściwa wartość atrybutu CUI, na podstawie ustaleń z p. 1 (odbywa się to w sekcji `post-auth` konfiguracji FreeRADIUS-a).

Jeżeli przewidujemy wysyłanie atrybutu CUI, to wskazane jest usunięcie atrybutu `User-Name` z odpowiedzi.

Serwery instytucji RADIUS pracujące w polskiej usłudze eduroam po podjęciu decyzji, że pakiet Access-Request ma zostać przekierowany do innego serwera, powinny dopisać do pakietu atrybut `Chargeable-User-Identity` z pustą wartością, jeśli nie ma już w nim atrybutu tego typu. W ten sposób serwer deklaruje chęć korzystania z mechanizmu CUI, niezależnie od możliwości urządzeń dostępowych. Niezbędne jest również dopisanie atrybutu Operator-Name z wartością „1nazwa_domenowa”. Nazwa domenowa jest domeną przypisana do instytucji, a cyfra 1 jest znacznikiem obszaru nazw stosowanym w Operator-Name (w tym przypadku jest to obszar 'nazwy domenowe').

5. Przykład rozwiązania wspomagającego obsługę incydentów

Poniżej opisujemy, jak można przygotować się do realizacji zadań związanych z rozwikłaniem incydentów sieciowych.

Przedstawione mechanizmy przechowywania danych usługi eduroam zostały oparte na usłudze syslog-ng i na bazie MySQL.

5.1. Ochrona przed zmianą adresu IP przez użytkownika

Gdy chcemy zagwarantować, by adres IP, po jego nadaniu konkretnemu adresowi MAC, nie został zmieniony samodzielnie przez zaradnego użytkownika, to należy przede wszystkim zapewnić ochronę dostępu do sieci w określonych przestrzeniach adresowych. Uzyskanie adresu IP przez klienta nie może dawać od razu prawa korzystania z otwartej sieci. Jeśli np. filtrujemy pakiety sieciowe za pomocą mechanizmu `iptables` i domyślnie klienci w VLAN-ie 11 nie mają otwartej sieci, to użytkownik o MAC-u `aa:bb:cc:dd`, który otrzymał adres `11.22.33.44` w tym VLAN-ie uzyska dostęp do sieci po dodaniu reguł:

```
-A FORWARD -s 11.22.33.44 -i vlan11 -o eth0
       -m mac --mac-source aa:bb:cc:dd -j ACCEPT
-A FORWARD -d 11.22.33.44 -i eth0 -o vlan11 -j ACCEPT
```

Przykładowa implementacja rozwiązania polegającego na ochronie przed samodzielną zmianą adresu IP przez użytkowników eduroam została opisana w dokumencie [4]. W przedstawionym podejściu zastosowano pakiet `dnsmasq`, realizujący funkcję serwera DHCP oraz przekierowującego DNS-a. Specyfiką serwera `dnsmasq` jest możliwość powiązania zdarzenia przydzielenia adresu sieciowego z wywołaniem wskazanego skryptu. Zadaniem tego skryptu jest otwarcie połączenia sieciowego dla danego klienta.

Obecnie analogiczną funkcjonalność można uzyskać korzystając z pakietu DHCPD.

Można również użyć funkcji wiązania adresów IP i MAC dostępnych w niektórych urządzeniach sieciowych takich jak przełączniki lub kontrolery bezprzewodowe.

5.2. Utrzymywanie logów DHCP

Serwer DHCP można skonfigurować tak, by zapis aktywności systemu był realizowany poprzez usługę `syslog`. Na ogół najwygodniej jest, by serwer DHCP logował do zdalnego serwera, dedykowanego do obsługi zapisów pracy zarówno DHCP, jaki i serwerów RADIUS. Jeśli obsługa logowania na takim serwerze jest realizowana w oparciu o system `syslog-ng`, to możemy zastosować odpowiednie filtry oraz skrypty, by zgodnie z potrzebą przetworzyć zapisy. Np.

```
source s_net_udp { udp(); };
filter f_eduroam { netmask( "11.22.33.44/255.255.255.255" ); };
destination                                                d_eduroam
{ program("/opt/local/scripts/eduroamlogger.pl"); };
log { source(s_net_udp); filter(f_eduroam);
      destination(d_eduroam); };
```

ustala, że jeśli źródłem logów jest serwer 11.22.33.44, to zostaje uruchomiony skrypt `/opt/local/scripts/eduroamlogger.pl`. Skrypt ten może dodatkowo zinterpretować dane wejściowe i na ich podstawie przygotować instrukcje SQL by załadować dane do bazy MySQL. W ten sposób dane dotyczące powiązania MAC – IP mogą być zapisywane w specjalnej tabeli bazy danych przeznaczonej do gromadzenia informacji o usłudze eduroam.

5.3. Zapisy uwierzytelniania

Jeśli w konfiguracji oprogramowania FreeRADIUS zdefiniowano blok `detail auth_log {...}`, to należy jedynie zadbać, by w sekcji `post_auth { ... }` znalazło się wskazanie `auth_log` (najlepiej blisko końca bloku, po instrukcjach modyfikujących zawartość pakietu odpowiedzi, by zapis logowania miał zawartość zgodną z przekazywaną klientowi).
FreeRADIUS pozwala również zdefiniować logowanie poprzez bazę SQL. Służy do tego sekcja `sql_log`, ustalająca konfigurację dla modułu `rlm_sql_log`. Zasada działania jest następująca:

1. moduł dopisuje instrukcje SQL do wskazanego pliku,
2. plik jest źródłem danych dla specjalnego programu pakietu FreeRADIUS – `radsqlrelay`.

Przykładowo kod:

```
sql_log {
 path = "${radacctdir}/sql-relay"
 postauth_table = "freeradiusauth"
 Post-Auth = "INSERT INTO ${postauth_table}                    \
  (user,cui,reply,nasip,cliip,called,calling,date,radius,vlan) VALUES
\
  ('%{User-Name}',        \
   '%{reply:Chargeable-User-Identity}',        \
   '%{reply:Packet-Type}', \
   '%{NAS-IP-Address}', \
   '%{Client-IP-Address}', \
       left(ucase(replace(replace(replace('%{Called-Station-Id}','-',
''),'.',''), ':', '')), 12), \
     left(ucase(replace(replace(replace('%{Calling-Station-Id}','-'  ,
''),'.',''), ':', '')), 12), '%S', \
   'radius1.umk.pl', '%{reply:Tunnel-Private-Group-Id}');"
}
```

powoduje, że do tablicy `freeradiusauth` zostanie zapisany rekord dotyczący danej sesji uwierzytelnienia. Rekord ten będzie zawierał informację, na jakim serwerze nastąpiło uwierzytelnienie. Zapasowy serwer powinien tak samo zapisywać informację do bazy SQL.

5.4. Korzystanie z mechanizmu Chargeable-User-Identity

Aby dostosować się do zaleceń polskiej usługi eduroam dotyczących przekazywania informacji o użytkownika, należy włączyć na serwerze RADIUS instytucji obsługę atrybutu `Chargeable-User-Identity`. Jeżeli urządzenia dostępowe, z których korzystamy nie mają funkcjonalności CUI, trzeba zagwarantować, by serwer przed przekierowaniem zlecenia dodał atrybut `Chargeable-User-Identity` o pustej wartości (zgodnie z [5]). Szczegółowy opis konfiguracji FreeRADIUS-a w celu korzystania z atrybutu `Chargeable-User-Identity` można znaleźć w dokumencie [6].

Materiały towarzyszące

[1] *eduroam Service Definition*, http://www.eduroam.pl/regulamin/GN3-12-192_eduroam-policy-service-definition_ver28_26072012.pdf

[2] *Polski regulamin eduroam*, http://www.eduroam.pl/regulamin/

[3] *Koncepcja wdrożenia usługi eduroam w sieci Pionier*, T. Wolniewicz, M. Górecka-Wolniewicz, Z. Ołtuszyk http://www.eduroam.pl/Dokumentacja/koncepcja_polska-1.0.pdf

[4] *Zabezpieczenie przez zmianą adresu IP przez Użytkownika,* A. Angowski, http://www.eduroam.pl/Dokumentacja/eduroam_zapobieganie_zmianie_IP.pdf

[5] *Chargeable User Identity*, F. Adrangi, A. Lior, J. Korhonen, J. Loughney, RFC 4372

[6] *Instalacja i konfiguracja serwera FreeRADIUS v.2*, M. Górecka-Wolniewicz, http://www.eduroam.pl/Dokumentacja/freeradiusv2-09-2012.pdf