Határidős accountok WiFi rendszerekhez

Pásztor György
pasztor@bibl.u-szeged.hu
Szegedi Tudományegyetem - Egyetemi Könyvtár

—

Bán Attila István
miham@bibl.u-szeged.hu
Szegedi Tudományegyetem - Egyetemi Könyvtár

Az előadás szerkezeti áttekintése

– A probléma és a körülmények specifikálása
– A probléma megoldásához használt eszközök
– A eszközök felhasználásának hogyanja

A probléma I.

A probléma: Adjunk a könyvtár használói számára drótnélküli internetelérést

Elvárások a rendszertől

- Biztonságos legyen
- A felhasználó számára egyszerűen telepíthető legyen
- Egyszerű legyen a hozzá kapcsolódó adminisztráció
- Illeszkedjen be a meglévő hálózati infrastruktúránkba
- Többféle WiFi accountot képesek legyünk kezelni

A probléma II.

Biztonság

Biztonsággal kapcsolatos kérdések:

- A forgalmazott adatokat ne lehessen ”road-warrior” eszközökkel lehallgatni
- Az accountokat lehetőség szerint, ne tudják egymástól ”ellopni”

Felhasználóbarátság

- Lehetőleg ne kelljen külön szoftvert telepíteni a laptopokra
- Gyorsan és könnyen beállítható legyen

A probléma III.

Egyszerű adminisztráció

– A hálózat vagy avval kapcsolatos konfigurációba ne kelljene belenyúlnia, csak a hálózat üzemeltetőinek és ne az accountot kiadó nem-technikai munkatársaknak.

– „kaparós sorsjegy” ötlet: Az igényeknek megfelelően legyártunk előre accountokat, amelyek az első használattól lépnek életbe, és egy megadott ideig élnek csak.

A probléma IV.

Az eddigi körülmények

– Adott egy hálózat az épületben (3750-es Routerek, és 2950-es Switchek)

– A hálózat üzemeltetéséhez adott egy radius szerver

– Adott a helyszín, ahol működnie kell: leárnyékolt részek, több emelet, stb.

Többféle account

– ,,Normál” lejárós accountok, korlátozott interneteléréssel

– ,,VIP” accountok, amelyek nem járnak le, korlátlan netelérésük van, stb.

Eszközök I.

Beléptetés 802.1X-el:

- MD5 auth elvetve, mert a windowsos kliensek SP után nem engedik
- kliens certificate elvetve, mert:
  - túl sok adminisztráció kellene a certek előállításához
  - a certificateket a laptopokra fel kell telepíteni, így nem kifejezetten felhasználóbarát
  - nehezebben oldható meg a lejáratása (gyakorlatilag egy user/passw párosra kihegyezett infrastruktúrát így is üzembe kellene hozzá helyezzünk)
- PEAP+mschapv2 lett a nyerő: szinte minden supplicant ismeri

Eszközök II.

Már adott eszközök, amiket felhasználtunk, kiegészítettünk

A freeradius már adott volt, mint radius szerver(authenticator)

- plain text fájlról átálltunk sql backendre, így ha egy új bejegyzést tettünk, nem kellett a radius szervert újraindítani
- A freeradius saját sql sémáit módosítva létre tudunk hozni olyan táblákat, amelyekbe bizonyos adatok dinamikusan jellennek meg az accountok élettartamától függően

Eszközök III.

A többféle accountok problémaköre

– A különböző típusú accountok különböző vlanokba (802.1Q trunking)

– A radius válaszban pedig megmondjuk, hogy melyik vlan-ba kerüljön a kliens

Egy AP felé néző port konfigja:

```
interface FastEthernet0/2
 switchport trunk native vlan 200
 switchport trunk allowed vlan 200,210,211,607
 switchport mode trunk
 no snmp trap link-status
 spanning-tree portfast
```

Eszközök IV.

A biztonság problémaköre

WPA, ill. legacy célokra dinamikus 128 bites WEP

- Változó WEP kulcs
- Kliensenként változik a kulcs (radius szervert igényel!)
- Az idő elteltével a kliensekhez rendelt kulcs helyett is újat generál

Részletek az AP konfigból:

```
interface Dot11Radio0
 encryption vlan 607 mode ciphers tkip wep128
 encryption vlan 211 mode ciphers tkip wep128
 encryption vlan 210 mode ciphers tkip wep128
 broadcast-key vlan 607 change 1200
 broadcast-key vlan 211 change 1200
 broadcast-key vlan 210 change 1200
 ssid GUEST
    vlan 210
    authentication open eap eap_methods
    authentication key-management wpa optional
    accounting acct_methods
```

Részletek II.:

```
ssid SZTE-EK
   vlan 211
   authentication open eap eap_methods
   authentication key-management wpa optional
   accounting acct_methods
   guest-mode
ssid SZTE-EK-VIP
   vlan 607
   authentication open eap eap_methods
   authentication key-management wpa optional
   accounting acct_methods
dot1x reauth-period 1200
```

Megoldás I.

A „lejáró” accountok

```
CREATE TABLE kvt_wifi_access (
    username text,
    start_time timestamp without time zone DEFAULT
      '1970-01-01 00:00:00'::timestamp without time zone,
    valid_period integer DEFAULT 0,
    expire_date timestamp without time zone DEFAULT
      '1970-01-01 00:00:00'::timestamp without time zone,
    id integer DEFAULT
      nextval('public.static_radcheck_id_seq'::text) NOT NULL
);
```

Megoldás II.

A lejáró accountok ellenőrzése

```
CREATE VIEW dynamic_radcheck AS
  SELECT kwa.id, kwa.username,
         'User-Password'::text AS attribute,
         '=='::text AS op,
         'guestwifi'::text AS value
  FROM kvt_wifi_access kwa;
```

Radius konfigmod (freeradius/postgresql.conf):

```
postauth_query = "UPDATE kvt_wifi_access SET start_time = 'now', \
    expire_date = now() + valid_period * interval '1 second' \
    WHERE   username = '%User-Name' \
      AND start_time = '1970-01-01'::timestamp;"
```

Megoldás III.

Minden radius attributum ellenőrzése

```
CREATE VIEW radcheck AS
  SELECT dynamic_radcheck.id, dynamic_radcheck.username,
         dynamic_radcheck.attribute, dynamic_radcheck.op,
         dynamic_radcheck.value
  FROM dynamic_radcheck
 UNION ALL
  SELECT static_radcheck.id, static_radcheck.username,
         static_radcheck.attribute, static_radcheck.op,
         static_radcheck.value
  FROM static_radcheck;
```

Megoldás IV.

A lejáró accountok csoportba sorolása

```
CREATE VIEW dynamic_usergroup AS
  SELECT 0 AS id, kwa.username,
     CASE WHEN ((kwa.expire_date = '1970-01-01 00:00:00'::timestamp
                 without time zone)
     OR ((kwa.expire_date)::timestamp with time zone > now()))
     THEN 'wifi'::text
     ELSE 'cage'::text END AS groupname
  FROM kvt_wifi_access kwa;
```

Megoldás V.

A csoportok összefésülése

```
CREATE VIEW usergroup AS
  SELECT dynamic_usergroup.id, dynamic_usergroup.username,
         dynamic_usergroup.groupname
  FROM dynamic_usergroup
 UNION ALL
  SELECT static_usergroup.id, static_usergroup.username,
         static_usergroup.groupname
  FROM static_usergroup;
```

Megoldás VI.

Klasszikus radius adminisztráció

A klasszikus radius bejegyzések:

```
INSERT INTO static_radcheck (username, attribute, op, value)
                VALUES ('pasztor', 'Auth-Type', ':=', 'Local');
...             VALUES ('pasztor', 'User-Password', '==', 's3cr3t');
...             VALUES ('miham', 'Auth-Type', ':=', 'Local');
...             VALUES ('miham', 'User-Password', '==', 's3cr3t2');
INSERT INTO radreply (username, attribute, op, value)
                VALUES ('pasztor', 'Service-Type', '=', 'Login-User');
...             VALUES ('miham', 'Service-Type', '=', 'Login-User');
```

Megoldás VII.

WiFi csoportok vsa attribútumai

wifi és vip csoport:

```
INSERT INTO radgroupreply (groupname, attribute, op, value)
        VALUES ('wifi', 'Service-Type', '=', 'Framed-User');
...     VALUES ('wifi', 'Tunnel-Type:1', '=', '13');
...     VALUES ('wifi', 'Tunnel-Medium-Type:1', '=', '6');
...     VALUES ('wifi', 'Tunnel-Private-Group-ID:1', '=', '210');

...     VALUES ('vip', 'Service-Type', '=', 'Framed-User');
...     VALUES ('vip', 'Tunnel-Type', '=', ':1:13');
...     VALUES ('vip', 'Tunnel-Medium-Type', '=', ':1:6');
...     VALUES ('vip', 'Tunnel-Private-Group-ID', '=', ':1:607');
```

Megoldás VIII.

vip&mac

eap.conf:

```
eap {
        default_eap_type = peap
...
        peap {
                default_eap_type = mschapv2
                copy_request_to_tunnel = yes
        }
...
}
```

Megoldás IX.

WiFi accountok managemntje

vip account:

```
INSERT INTO static_radcheck (username, attribute, op, value)
     VALUES ('vip00','User-Password','==','vippw00');
...  VALUES ('vip00','Calling-Station-Id','==','0003.1b57.a443');
INSERT INTO static_usergroup (username, groupname)
     VALUES ('vip00','vip');
```

nem vip account:

```
INSERT INTO kvt_wifi_access (username, start_time,
                             valid_period, expire_date)
     VALUES ('hSjZI1GLlmPU', '1970-01-01 00:00:00',
             345600, '1970-01-01 00:00:00');
```

online cím:

`http://www.bibl.u-szeged.hu/~pasztor/nws2k6/`