RadSec a IPsec

metody zabezpečeného připojení k národnímu RADIUS serveru

Jan Tomášek <jan.tomasek@cesnet.cz>

CESNET, z. s. p. o.
Zikova 4
Praha 6

IPsec - shrnutí

+ standartizované řešení od roku 1998, RFC 2401
+ implementováno na většině platform
  - *BSD
  - Linux
  - Solaris
  - MS Windows
+ provozujeme +/- úspěšně od 3Q 2004

+/- pracuje na 3. vrstvě OSI modelu (sítová vrstva)
  => aplikace si nemůže být jistá že komunikuje bezpečně
  => aplikaci do toho nic není, zabezpečení komunikace má nastarosti kernel

- další IP prokololy (ESP, AH) které je nutné povolit na FW
- absence nástrojů pro diagnostiku problémů na lince (ping, traceroute, ...)
- mizerné logy *racoona* (Linuxový IKEY daemon)
- pro některé administrátory zcela nová věc

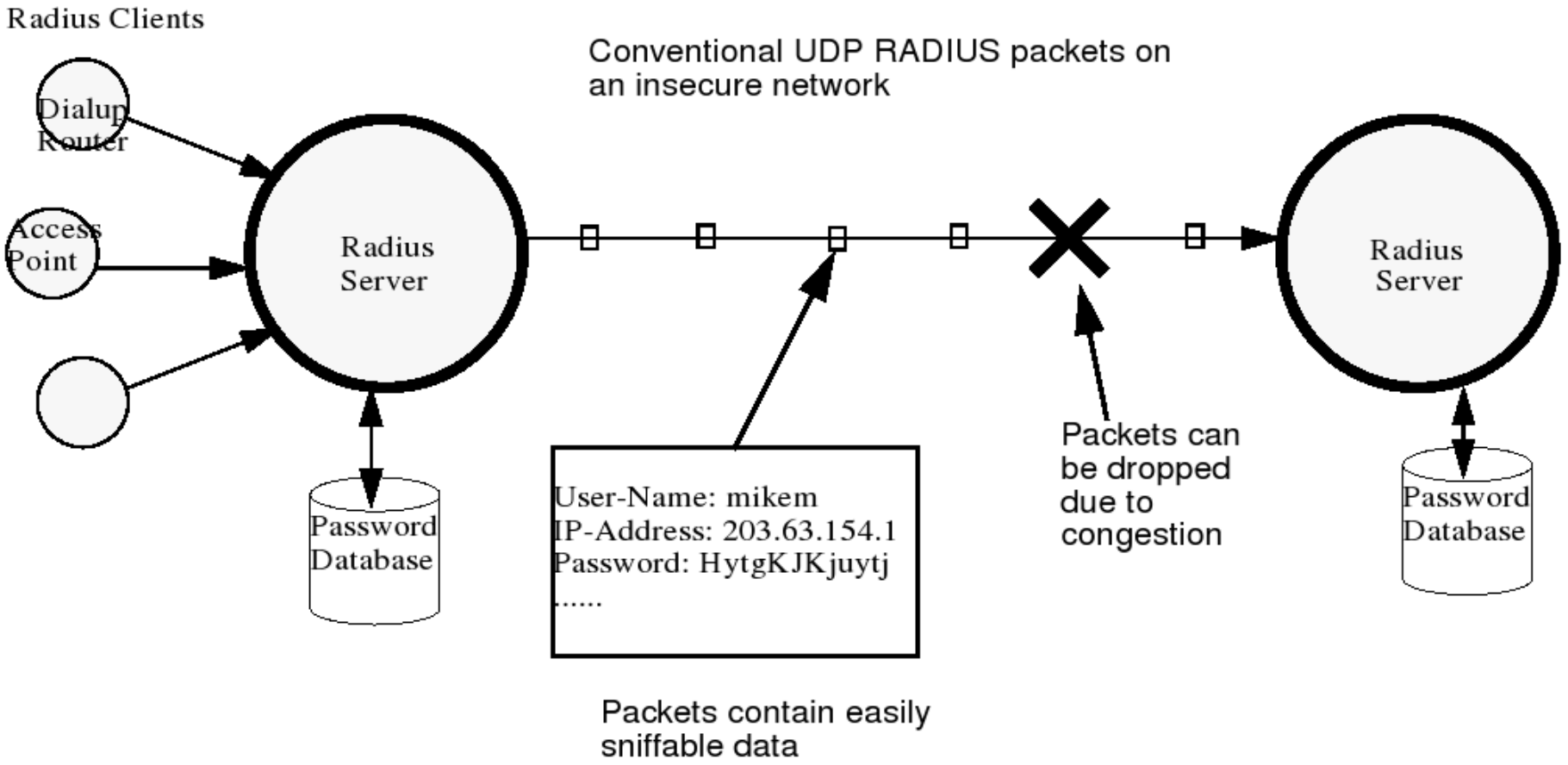
RadSec - úvod

- implementováno pouze v jediném RADIUS serveru a to v Radiatoru (od roku 2006
  - autory návrhu jsou OSC - autoři Radiatoru (http://www.open.com.au/radiator/radsec-whitepaper.pdf)
- "sem tam" nasazeno, ale bez detailního testování (mě to funguje...)

+/- pracuje na aplikační úrovni
  - když to RADIUS server neumí, tak má "smůlu"? NE! Ale...
+ používá TCP jako transportní protokol
  - o proti UDP se ví předem o tom že spojení nefuguje
+ zabezpečení pomocí TLS
  - s tím má každý zkušenosti

+ probíhající standartizace IETF (http://www.ietf.org/internet-drafts/draft-winter-radsec-01.txt)
+ Alan DeKok je ochoten to implementovat do FreeRADIUSu
+ *radsecproxy* (http://software.uninett.no/radsecproxy/)
  - lze vložit před jakýkoliv server
  - primárně Linux, lze ji ale přeložit i na Windows
  - sama osobě schopna pracovat jako proxy RADIUS server
  - Stig Venaas je vstřícný autor
  - software je stále ve vývoji

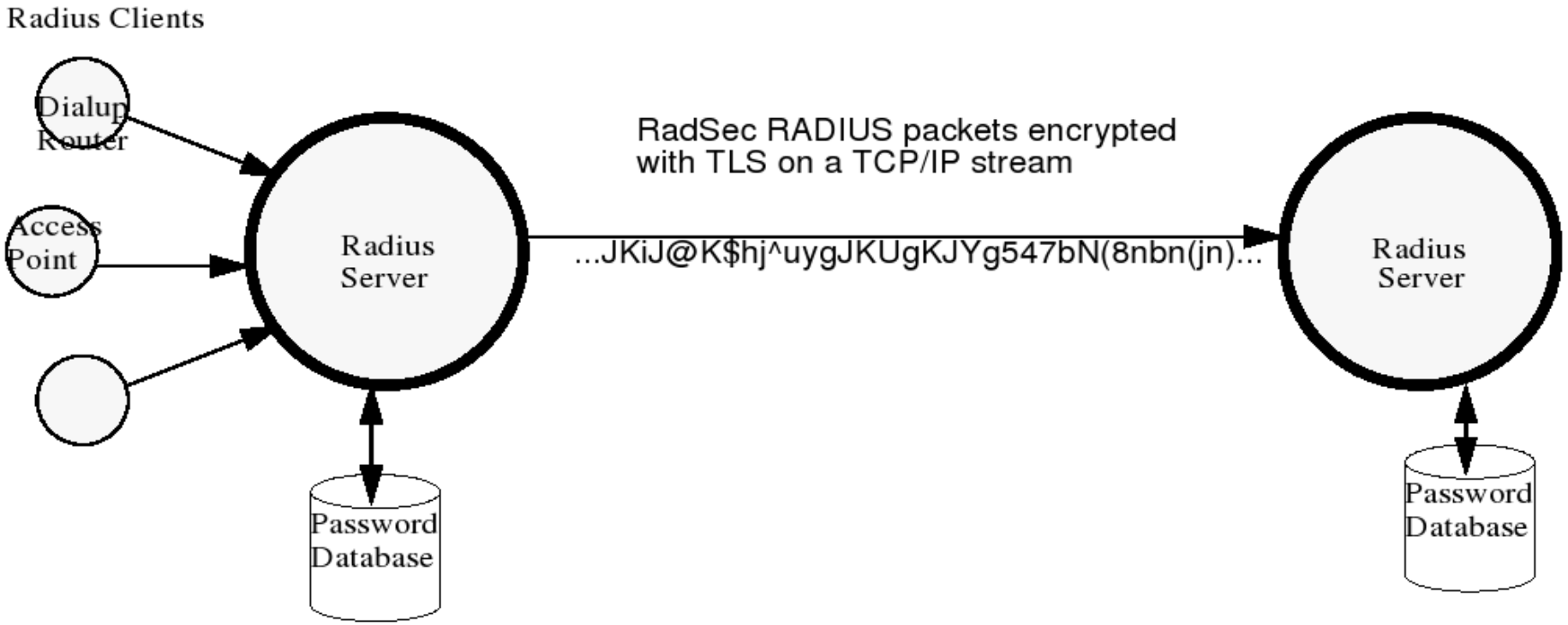
Problémy přenosu RADIUS paketů pomocí UDP



- pakety lze snadno odchytit, šifrováno je pouze heslo
- ztráta paketů je detekována je po timeoutu při čekání na odpověď

obrázek převzat z RadSec white paper od OSC

Výhody přenosu RADIUS paketů pomocí TCP



+ pakety nelze snadno dešifrovat - používá se silné šifrování
+ absence TLS spojení je známa před odesíláním dat
  + vylepšený přechod na záložní server
  - Radiator nevyužívá výhody TCP dostatečně
  + radsecproxy ano (plus Server-Status jako keep alive)

obrázek převzat z RadSec white paper od OSC

definice serveru – pro příchozí TCP spojení

definice klienta – pro odchozí TCP spojení

```
radius1:~# netstat -tn |grep 195.113.187.22
tcp        0      0 195.113.144.226:43619   195.113.187.22:2083     ESTABLISHED
tcp        0      0 195.113.144.226:2083    195.113.187.22:47100    ESTABLISHED
```

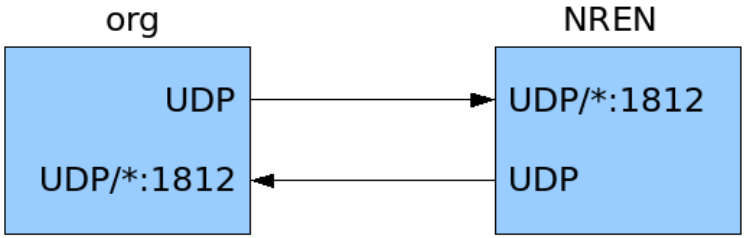
tj. pro každý protějšek budou existovat dvě spojení. Jedno pro příchozí (server) data druhé pro odchozí (klient) data.

```
<ServerRADSEC>
    Secret                  mysecret

    UseTLS
    TLS_CAPath              /etc/ssl/certs
    TLS_CertificateFile     /etc/ssl/certs/ipsec_certifikat.crt.pem
    TLS_CertificateType     PEM
    TLS_PrivateKeyFile      /etc/ssl/private/ipsec_certifikat.key.pem

    TLS_RequireClientCert

    TLS_CRLCheck
    TLS_CRLFile             /etc/ssl/certs/9b59ecad.r0
    TLS_SubjectAltNameURI   radius1.eduroam.cz
</ServerRADSEC>
```

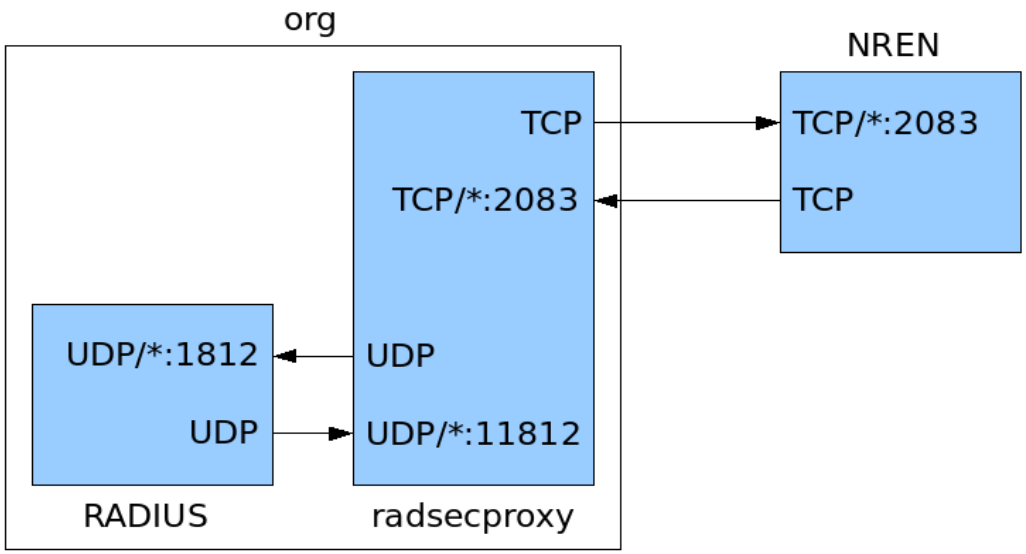
Konfigurace RadSec v Radiatoru

```
<Handler Realm=/^.+$/>
    <AuthBy RADSEC>
        Host                    radius1.eduroam.cz
        Secret                  mysecret

        MaxFailedRequests       2
        MaxFailedGraceTime      0
        FailureBackoffTime      0

        UseTLS

        TLS_CAPath              /etc/ssl/certs
        TLS_CertificateFile     /etc/ssl/certs/ipsec_certifikat.crt.pem
        TLS_CertificateType     PEM
        TLS_PrivateKeyFile      /etc/ssl/private/ipsec_certifikat.key.pem

        TLS_CRLCheck
        TLS_CRLFile             /etc/ssl/certs/9b59ecad.r0
        TLS_SubjectAltNameURI   radius1.eduroam.cz

        ReplyHook               file:"/etc/radiator/check_reply.pl"
    </AuthBy>

    AddToReplyIfNotExist        Tunnel-Private-Group-ID=1:100
    AddToReply                  Tunnel-Type=1:VLAN, \
                                Tunnel-Medium-Type=1:Ether_802
</Handler>
```

Klasické propojení RADIUS serverů po UDP



Propojení RADIUS serverů pomocí *radsecproxy*



```
tls default {
    CACertificatePath      /etc/ssl/certs
    CertificateFile        /etc/ssl/certs/ipsec_certifikat.crt.pem
    CertificateKeyFile     /etc/ssl/private/ipsec_certifikat.key.pem
}
server localhost {
        port    1812
        type    udp
        secret  mysecret
#        statusserver on
}
ListenUDP       localhost:11812
client  localhost {
        type    udp
        secret  mysecret
}
client radius1.eduroam.cz {
    typetls
    secret   mysecret
}
server radius1.eduroam.cz {
        type    tls
        secret  mysecret
#        statusserver on
}
realm lokalni-realm.cz {
        server localhost
}
realm * {
        server  radius1.eduroam.cz
}
```

Je třeba upravit `realm DEFAULT` **v souboru** `proxy.conf`**. Místo** `radius1.eduroam.cz:1812` **zadejte** `localhost:11812`**.**

```
realm DEFAULT {
        type                    = radius
        authhost                = localhost:11812
        secret                  = mysecret
        nostrip
}
```

Dále je třeba upravit soubor `clients.conf` **a přidat do něj sekci definující *radsecproxy* jako lokálního klienta.**

```
client localhost {
        secret          = mysecret
        shortname       = radsecproxy
}
```

Už testují:

* **TUL.CZ – Petr Adamec**; Radiator – oba servery
* **CUNI.CZ – Ladislav Fikais**; radsecproxy + FreeRADIUS – druhý server
* FEL.CVUT.CZ – Jiří Cejp; radsecproxy + FreeRADIUS – připravovaný druhý server
* VSB.CZ – Martin Pustka; Radiator – připravovaný záložní server

---

Radiator:

* možno nasadit do ostrého provozu
* pro nově příchozí jednoznačně preferovaná varianta

radsecproxy + FreeRADIUS:

* od verze 223 opravena kritická chyba způsobující segfault při odpojení protějšku
* zatím nereprodukovaný problém způsobující deadlock
* preferováno testování zkušeným administrátorem případně vývojářem v C

radsecproxy + nějaký Windows RADIUS server:

* zcela neotestováno
* preferováno testování vývojářem v C se zkušenostmi programování na UNIXových platformách - CygWin

Dotazy?

Děkuji za pozornost.

Dokumentace:

eduroam.cz: http://www.eduroam.cz/doku.php?id=cs:spravce:pripojovani:radsec:uvod

Odkazy:

Radiator: http://www.open.com.au/radiator/
RadSec White Paper: http://www.open.com.au/radiator/radsec-whitepaper.pdf
RadSec IETF Draft: http://www.ietf.org/internet-drafts/draft-winter-radsec-01.txt
radsecproxy: http://software.uninett.no/radsecproxy/
FreeRADIUS: http://www.freeradius.org/