CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA

Sigurnost na granici vaše mreže
OpenVPN i NuFW

Albert Novak – CARNet

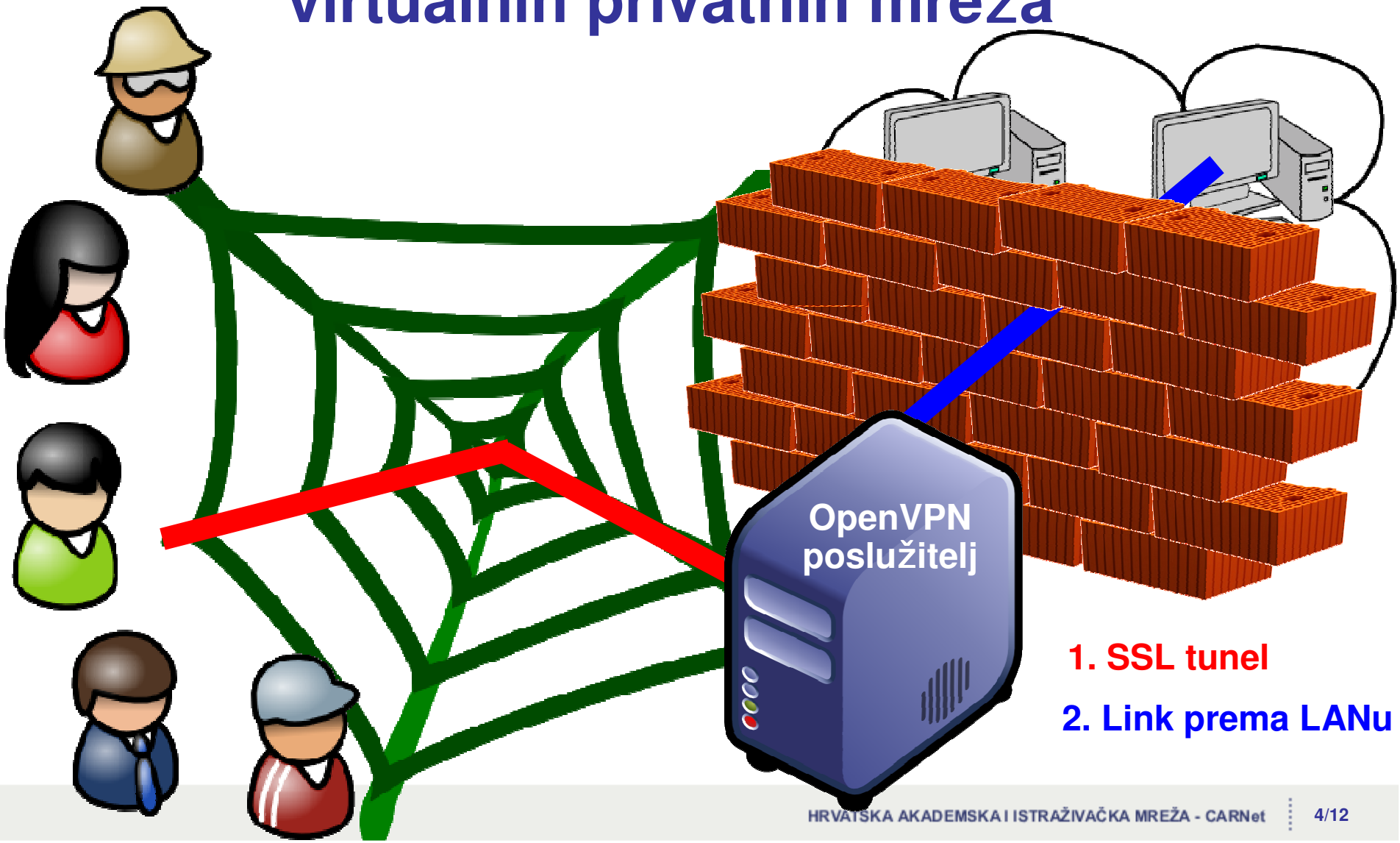
CUC 2007, 18.-20.11.2007.

Sadržaj

- Kako uspostaviti sigurnost na granici mreže?
- OpenVPN kao rješenje za uspostavu virtualnih privatnih mreža
- NuFW – fleksibilniji vatrozid
- Autentikacija i autorizacija bazirana na AAI@EduHr infrastrukturi
- Praćenje aktivnosti korisnika u slučaju sigurnosnih incidenata

Kako uspostaviti sigurnost na granici vaše mreže?

OpenVPN kao rješenje za uspostavu virtualnih privatnih mreža



OpenVPN

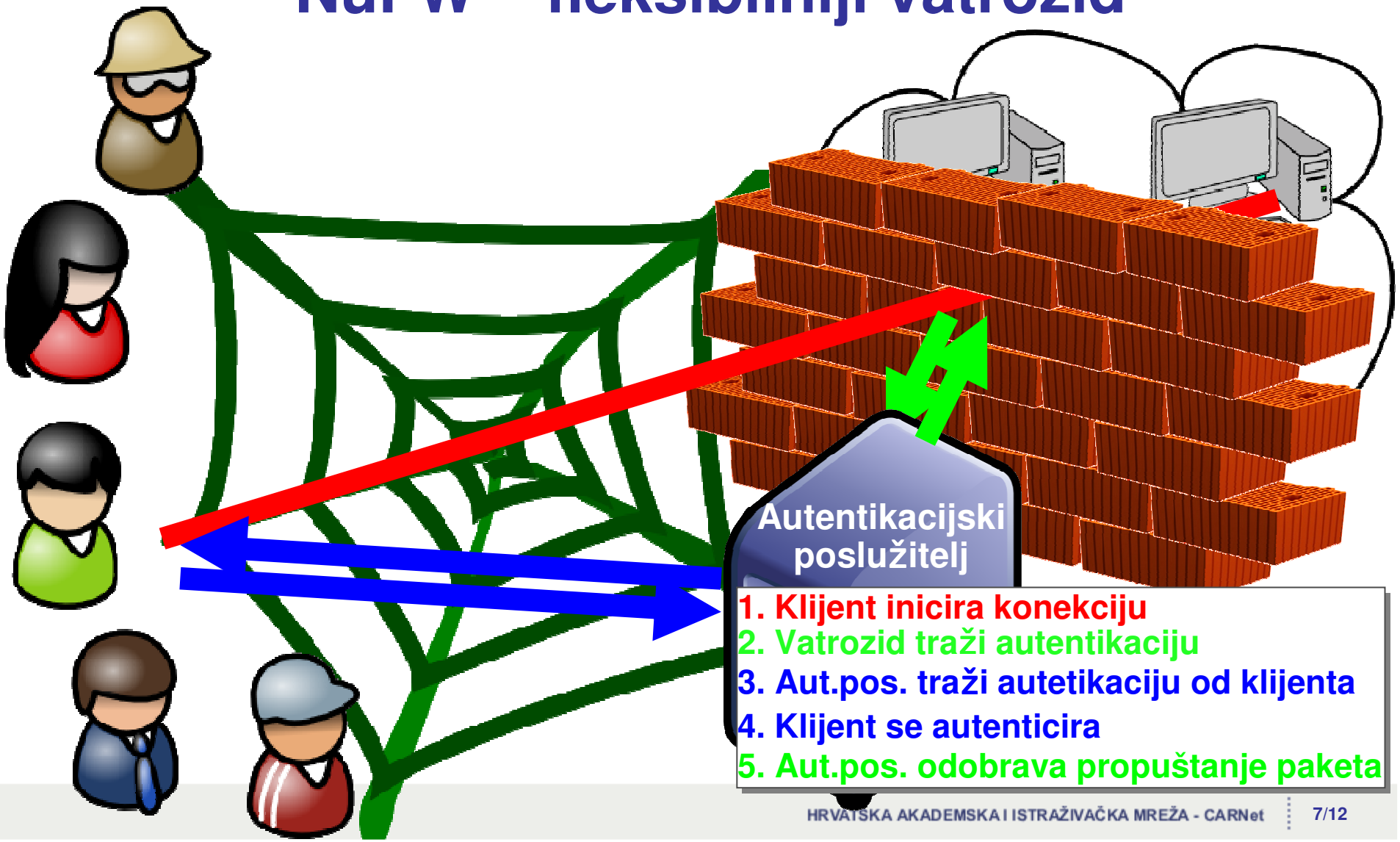
- Ne koristi IPsec vec je baziran na SSL/TLS-u
- Jednostavan za instalaciju, mogućnost redundancije i raspodjele opterećenja
- Koristi UDP/TCP port za komunikaciju klijenta i poslužitelja
- Za komunikaciju koristi virtualna mrežna sučelja tun (routing) i tap (bridging)
- Enkripcija i kompresija prometa kroz tunel
- OpenVPN poslužitelj može klijentu poslati rute (uključujući i defaultnu), DNS poslužitelj
- Mogućnost "personalizacije" konfiguracije u odnosu na klijenta koji pristupa
- Sučelje za upravljanje OpenVPN poslužiteljem
- Postoje klijenti za razne operacijske sustave - portabilan

OpenVPN – primjer konfiguracijske datoteke

```
#OpenVPN server
;local 192.168.0.1
port 1194
proto udp
dev tun
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/server.crt
key /etc/openvpn/keys/server.key
server 10.255.52.0 255.255.255.0
push "route 172.168.52.0 255.255.255.0"
push "redirect-gateway"
push "dhcp-option DNS 172.168.52.5"
cipher BF-CBC        # Blowfish (default)
comp-lzo
persist-key
persist-tun
max-clients 50
management localhost 7505
```

```
#OpenVPN client
client
dev tun
proto udp
remote 161.52.47.66
;remote-random
resolv-retry infinite
nobind
;user nobody
;group nobody
persist-key
persist-tun
ca ca.crt
cert client1.crt
key client1.key
cipher BF-CBC
comp-lzo
auth-user-pass
```

NuFW – fleksibilniji vatrozid



NuFW – fleksibilniji vatrozid

- Baziran na iptables-ima
- Omogućava donošenje odluke o propuštanju paketa na osnovu korisnika, a ne IP adrese
- Omogućava autwntikaciju kroz LDAP i PAM
- Omogućava fino podešavanje pravila o korisničkim pravima kroz ACL i to po:
  - protokolima, adresama i protovima koje propušta
  - vremenskom periodu
  - aplikaciji i OS-u
- Logiranje aktivnosti korisnika u tekstualne datoteke ili baze podataka
- ACL (Access Liste) u datotekama ili LDAP-u
- Potreban poseban klijent: Linux, MacOS i Windows (komercijalan)

NuFW – primjer ACL datoteke

```
# [Sample ACL] - /etc/nufw/acls.nufw
# decision=1            # decision if the rule matches (default: 0)
# gid=100,101           # which groups are concerned
# gid=103               # several lines can be used
# proto=6               # TCP (only 1 proto allowed per ACL, of course)
# type=0                # Type, for ICMP protocol only
# SrcIP=10.10.0.1       # Source IP, equivalent to 10.10.0.1/32
# SrcPort=1024-65535    # List of source ports (a single port is ok)
# DstIP=10.10.0.5       # Destination IP address
# DstIP=10.10.0.8, 10.10.1.0/24 # There can be several IP addresses/lines
# DstPort=5150-5153     # List of destination ports
# DstPort=22,25         # There can be several lines

[ssh]
decision=1
gid=100
proto=6
SrcIP=0.0.0.0/0
SrcPort=1024-65535
DstIP=0.0.0.0/0
DstPort=22
App=/usr/bin/ssh
OS=Linux
period=8-16
```

```
#/etc/nufw/periods.xml
<period name="8-16" desc="work hour">
   <perioditem>
      <hours start="8" end="18"/>
   </perioditem>
</period>
<period name="interval" desc="one hour interval">
   <perioditem>
      <duration length="3600"/>
   </perioditem>
</period>
```

Autentikacija bazirana na AAI@EduHr infrastrukturi

- Ideja je iskoristiti AAI@EduHr infrastrukturu za autentikaciju korisnika koji koriste OpenVPN poslužitelj i NuFW vatrozid
- OpenVPN
  - autentikacija korisničkim imenom i zaporkom
  - pristup AAI@EduHr infrastrukturi putem radius PAM modula
- NuFW
  - zahtjeva sitnu promjenu u kodu
  - dodatni NSS (Name Service Switch) modul za defaultne postavke korisnika
  - koristi radius PAM modul

Autentikacija bazirana na AAI@EduHr infrastrukturi - OpenVPN

- Potrebno je dodatno instalirati
  - radius pam modul: apt-get install libpam-radius-auth
  - s debian paketom openvpn već dolazi openvpn-auth-pam modulom

OpenVPN poslužitelj - 161.53.47.66

```
#/etc/openvpn/server.conf
plugin /usr/lib/openvpn/openvpn-auth-pam.so
radproxy
client-cert-not-required
username-as-common-name
```

```
#/etc/pam.d/radproxy
auth    required        pam_radius_auth.so debug
```

```
#/etc/pam_radius_auth.conf (
# server[:port] shared_secret      timeout (s)
161.53.47.67     zaporka         5
```

RADIUS poslužitelj - 161.53.47.67

```
#/etc/freeradius/radius.conf
client 161.53.47.66 {
        secret     = zaporka
        shortname = OpenVPN
}
```

Autentikacija bazirana na AAI@EduHr infrastrukturi - NuFW

- Potrebna je minimalna izmjena nuauth system modula izvornog koda
- Dodatni NSS modul za definiranje defaultnog korisnika - libnss-ato

NuAuth poslužitelj - 161.53.47.66

```
#/etc/nufw/nuauth.conf
nuauth_user_check_module="system"
nuauth_get_user_id_module="plaintext system"
nuauth_get_user_groups_module="plaintext
system"
```

```
#/etc/nsswitch.conf
passwd:         compat ato
group:          compat
shadow:         compat ato
```

```
#/etc/pam.d/nuauth
auth    required        pam_radius_auth.so debug
```

```
#/etc/pam_radius_auth.conf (
# server[:port] shared_secret      timeout (s)
161.53.47.67     zaporka         5
```

RADIUS poslužitelj - 161.53.47.67

```
#/etc/freeradius/radius.conf
client 161.53.47.66 {
        secret    = zaporka
        shortname = OpenVPN
}
```

Praćenje aktivnosti korisnika u slučaju sigurnosnih incidenata

- Bazirano na mogućnostima iptablesa za praćenjem konekcija
  - LOG i ULOG
- NuFW može podatke o konekcijama slati NuAuth-u koji ih može spremati u bazu
- Postoje alati za prikaz takvih podataka:
  - nulog i nulog2
  - logwatch
- Trenutno stanje:
  - nutop
  - iptstate

I na kraju ...

- OpenVPN
  - omogućava kreiranje sigurnih tunela kao između dviju mreža, tako i za road-warriore
  - baziran na SSL/TLS
  - jednostavna uspostava
- NuFW
  - napuštanje ideje klasičnih vatrozida: korisnik == IP
  - fleksibilnije podešavanje vatrozida
  - baziran na iptablesima
- Oba se daju integrirati s AAI@EduHr infrastrukturom
- Za generiranje poslužiteljskih certifikata iskoristite CARNetov SCS servis

... i još par linkova

- OpenVPN - http://openvpn.net/
- NuFW - http://www.nufw.org/
- Netfilter/IPtables - http://www.netfilter.org/
- INL Software - http://software.inl.fr/trac/trac.cgi/wiki
- libnss-ato - http://www.dm.unibo.it/~donatini/admin/libnss_ato/
- AAI@EduHr - http://www.aaiedu.hr