OpenVPN

Ondřej Caletka

3. března 2013

Virtuální privátní sítě

- Vytvoření privátní sítě nad veřejnou infrastrukturou.
- Například propojení privátních lokálních sítí prostřednictvím veřejné sítě Internet. (Site-to-site VPN)
- Nebo připojení pracovní stanice na cestě do privátní organizace. (Road warrior VPN)
- Dvě základní komponenty VPN:
  - šifrování
  - tunelování

Internet Protocol Security (IPsec)

- Způsob zabezpečení TCP/IP protokolu podle IETF.
- Vyvinut pro IPv6, portován do IPv4.
- Šifrování a autentizace od transportní vrstvy výše.
- Transportní i tunelovací režim.
- Nové protokoly pro výměny klíčů.
- Problémy s NATy a firewally.
- Jeho čas ještě přijde.

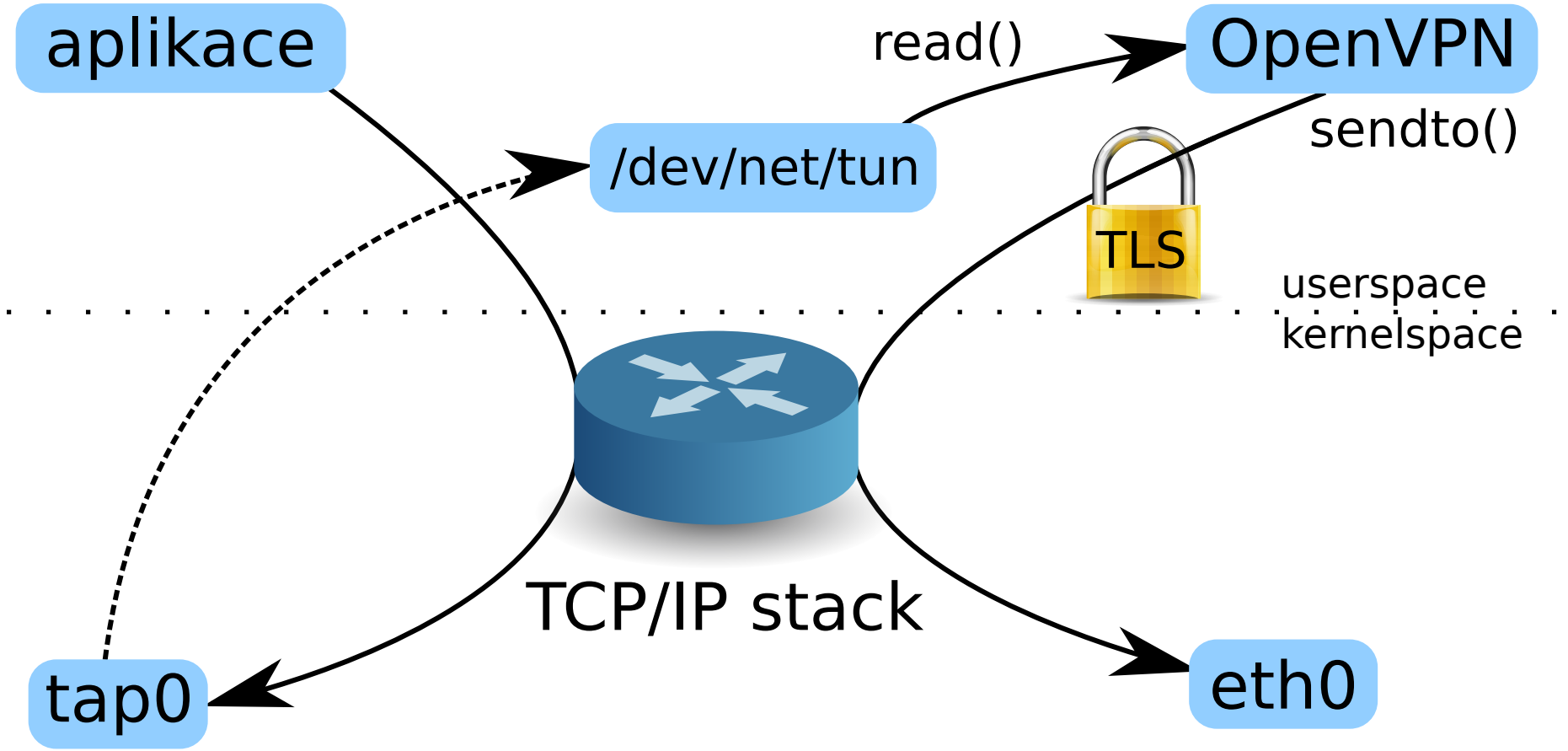
CESNET

OpenVPN

- Idea: Použít lety prověřenou mezivrstvu TLS (dříve SSL) namísto IPsec.
- Do TLS proudu se namísto aplikačních dat zapouzdřuje tunelovaný síťový provoz.
- Používá jeden UDP nebo TCP port.
- Přátelský k NATům a firewallům.
- Režim point-to-point, nebo point-to-multipoint.
- Použití TLS je volitelné.
- Špatná podpora IPv6 (do verze 2.2)

CESNET

Princip OpenVPN



Konfigurační volby

UDP nebo TCP?

- Pro správnou funkci je nutné UDP.
- Použití TCP vede k TCP-in-TCP problému.
- TCP se dá používat jen na kapacitních linkách.

TUN nebo TAP?

- Rozhraní `tap` představuje virtuální ethernet.
- Tun je efektivnější, ale umí jen IPv4 a IPv6.
- V případě multipoint režimu obsahuje OpenVPN buď switch (`tap`), nebo router (`tun`).
- Androidí klienti bez root oprávnění umějí jen `tun`.

Zapojení VPN do sítě

Bridged VPN

- VPN je přímo propojena s fyzickým segmentem.
- Fungují všechny protokoly.
- Šíří se broadcasty.
- Je třeba použít `tap` rozhraní.

Routed VPN

- Pro VPN slouží samostatný segment.
- Přenáší mezi fyzickou sítí a VPN je router.
- Lepší možnosti firewallingu.

Point-to-point VPN

```
# openvpn --dev tap --remote node2.example.com 1194
# openvpn --dev tap --remote node1.example.com 1194
```

Také je možná varianta server-klient (pro NATy):

```
# openvpn --dev tap
# openvpn --dev tap --remote server.example.com --nobind
```

Výše uvedené příklady nepoužívají šifrování. Pro PSK šifru vygenerujeme klíč:

```
# openvpn --genkey --secret /path/to/secret.key
```

Klíč přeneseme na obě strany a ke všem příkazům přidáme přepínač `--secret`.

TLS režim

- Oba účastníci vlastní X.509 certifikát a klíč.
- Také mají certifikát CA, která vydala účastnické certifikáty.
- Pomocí certifikátů si účstnící navzájem prokáží totožnost.
- Sdílený klíč se automaticky mění.
- Není třeba používat *pravé* certifikáty od komerčních autorit. Ostatně nechcete do sítě pouštět všechny majitele platných certifikátů.


I WILL MAKE MY OWN
CERTIFICATE AUTHORITY
WITH
BLACKJACK AND HOOKERS

Easy-RSA

Součástí OpenVPN je balík skriptů, které maximálně zpříjemňují práci s X.509 certifikáty pro potřeby OpenVPN.

`https://github.com/OpenVPN/easy-rsa`

```
$ cd /path/to/easy-rsa
$ source vars
$ ./clean-all
$ ./build-ca
$ ./build-key-server vpnserver.example.com
$ ./build-dh
$ ./build-key roadwarrior1
```

Multipoint TLS VPN

Konfigurace serveru

```
dev tap
server 10.20.30.0 255.255.255.0
dh /path/to/dh1024.pem
ca /path/to/ca.pem
cert /path/to/server.example.com.crt
key  /path/to/server.example.com.key
```

Konfigurace klienta

```
dev tap
client
remote server.example.com 1194 udp
ca /path/to/ca.pem
cert /path/to/roadwarrior1.crt
key  /path/to/roadwarrior1.key
ns-cert-type server
```

Remote provisioning

- VPN koncentrátor dokáže posílat příkazy klientům: `--push "redirect-gateway def1"`
- Přidělí adresy, DNS, nastaví směrování.
- Možnost vynutit přesměrování default GW.

Přesměrování brány

1. Je přidána host route směrem k VPN koncentrátoru.
2. Původní brána je nahrazena nebo překryta VPN.

Co se stane, když spadne fyzické rozhraní, kterým prochází VPN provoz?

Další možnosti

- Je možné nastavit `keepalive` pro udržování NATu a detekci nefunkčnosti.
- Server může dodatečně autentizovat klienty jménem a heslem.
- Server udržuje seznam přidělených adres a CN z certifikátů.
- Je možná speciální konfigurace pro klienta (například přidání směrovacího záznamu pro site-to-site VPN)

Pozvánka na workshop

- Postavíme P2P VPN mezi dvojicemi PC.
- Rozjedeme dynamické směrování s OSPF.
- Pokusíme se vytvořit co nejdelší traceroute. :)

Závěr

Děkuji za pozornost.