Tinc VPN - jak snadno najít toho pravého

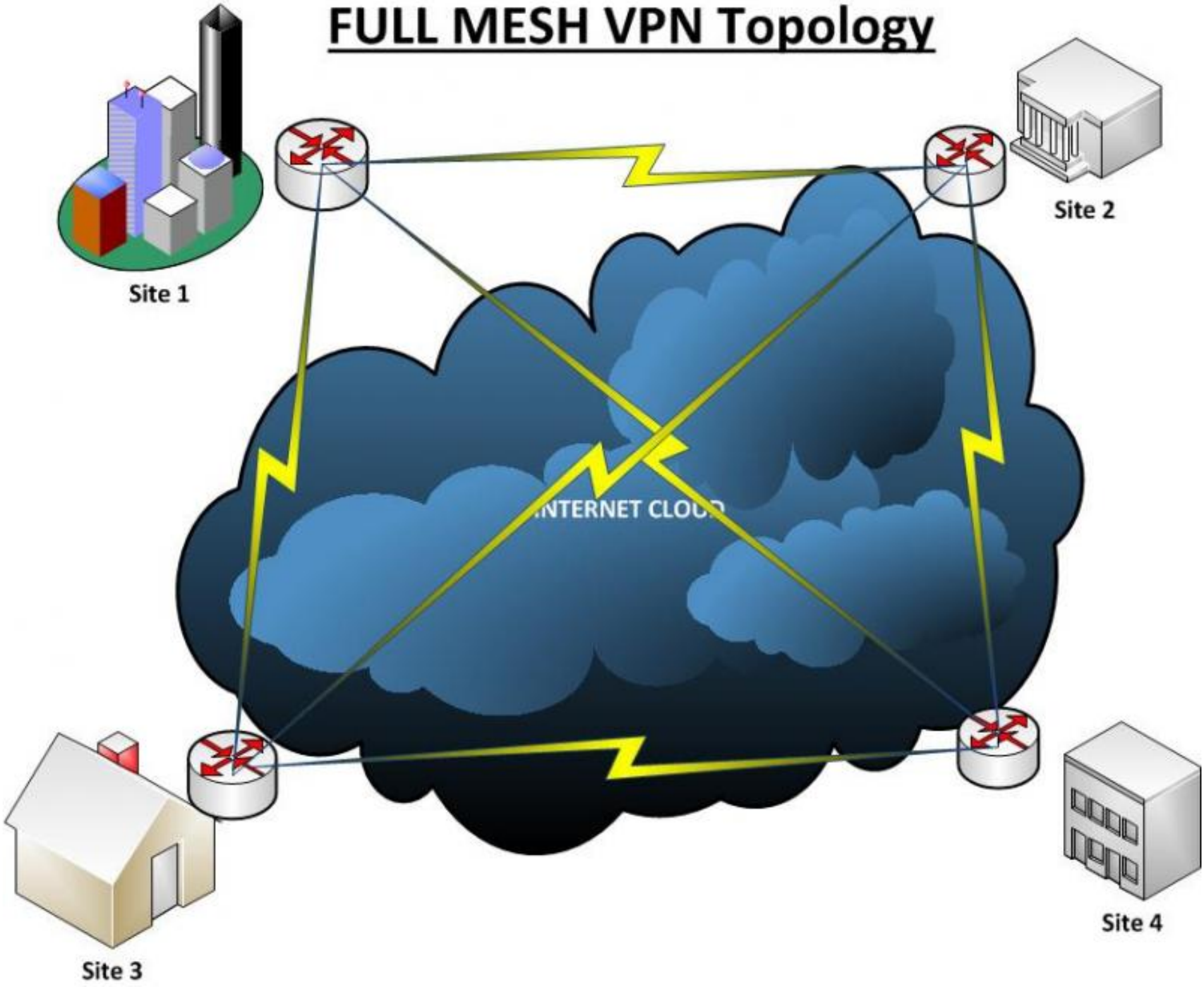
Michal Halenka
COEX s.r.o. / vpsFree.cz

tinc

VPN:

- IPsec2
    - tunnel only
- PPTP (*point-to-point* tunelling protocol)
- OpenVPN
    - point to multipoint
    - mesh pro *n* nodů => *n+1* konfigurací
- (Hamachi)/LogMeIn a další proprietární technologie

FULL MESH VPN Topology



O TINC VPN

- první vydání z 1998 (vpnd)
- novinky v nestabilních verzích 1.1 (invite, SPTPP, ...)
- postaveno na OpenSSL/LibreSSL, zlib a LZO
- podpora v *BSD, OpenWRT, Androidu, iOS, Solaris(sparc32), Darwin, Windows ...
- l2 nebo L3 režím
- IPv6 podpora
- podpora více VPN sítí

- decentralizováno
- endpointy, tinc udělá zbytek
- VPN přes UDP, fall-back to TCP pokud UDP neprojde
- metadata přes TCP

tinc

NAT traversal:

- změny source addr a portu
- blokované příchozí spojení
-
- možná řešení:
- routování mimo - neefektivní
- port forwarding - vyžaduje konfiguraci
- UPnP - komplexí, vyžaduje podporu routeru
- výměna informací o dest portu jaký se má použít (STUN)

Příklad: náhrada OpenVPN

Nastavení lokálního stroje:

```
/etc/tinc/nets.boot
    moje_vpn
/etc/tinc/moje_vpn/tinc.conf:
    Name = vpn_server1
    AddressFamily = ipv4
    Interface = tun0
root@server:/# tincd -n vpn_server1 -K 4096
    ... /etc/tinc/moje_vpn/rsa_key.priv
    ... /etc/tinc/moje_vpn/hosts/vpn_server1
$ echo "Subnet = 10.0.0.8/32" >> /etc/tinc/moje_vpn/hosts/vpn_server1
$ echo "Address = 83.167.228.42" >> /etc/tinc/moje_vpn/hosts/vpn_server1
/etc/tinc/moje_vpn/tinc-up
    #!/bin/sh
    ifconfig tun0  10.0.0.8 netmask 255.255.255.0
/etc/tinc/moje_vpn/tinc-down
    #!/bin/sh
    ifconfig tun0 down
```

Příklad: náhrada OpenVPN

Zkopírovat /etc/tinc/moje_vpn/hosts/* ze všech nodů na všechny nody

```
root@vps1:/etc/tinc# tree
.
├── nets.boot
└── moje_vpn
    ├── hosts
    │   ├── vpn_server1
    │   ├── vpn_client1
    │   ├── vpn_client2
    │   └── vpn_client3
    ├── rsa_key.priv
    ├── tinc.conf
    ├── tinc-down
    └── tinc-up
```

Prostor pro otázky