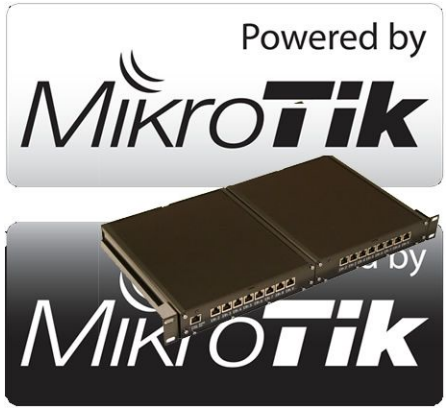
VPN TUNELI

DIZAJN I PRIMENA KOD MIKROTIK UREĐAJA



Predavač : Zoran Antončić

Protokol
Skup pravila za slanje podataka kroz mrežu

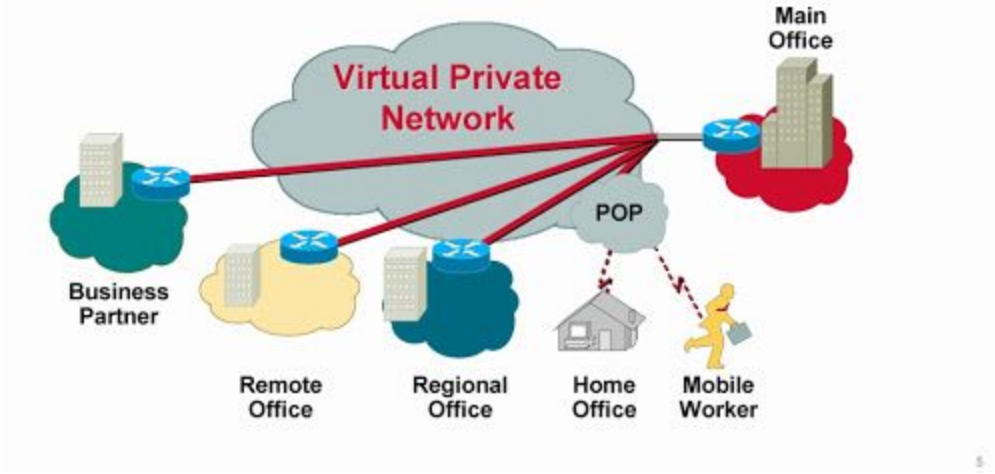
Interfejs
Komponenta mrežnog uredjaja
L2 I L3
Layer 2 i Layer 3 OSI modela
L2 – data link – prijem i prenos paketa putem mediuma
L3 – network – servis kroz rutiranje IP adresiranje

Redudantnost
Više veza ka lokaciji- backup veza
Dekapsulacija i enkapsulacija
Pakovanje i raspakivanje podataka

VPN – VIRTUAL PRIVATE NETWORK

-VPN je (ne)sigurna konekcija preko intenteta koja služi sa povezivanje više lokacija sa korporativnom mrežom

- povezivanje udaljenih lokacija
- povezivanje kućnih korisnika
- povezivanje mobilnih korisnika



Mikrotik je Letonski prozvođač mrežne opreme koji u svojoj ponudi nudi širok spektar aktivne I pasivne opreme.

Mikrotik je ustvari OS koji se ugradjuje u ,,routerbordove”

-Kao OS mikrotik nudi veliki broj mogućnosti rada uredjaja kao sto su :
- Rutiranje i switching
- Firewall
- VPN
- Proxy …

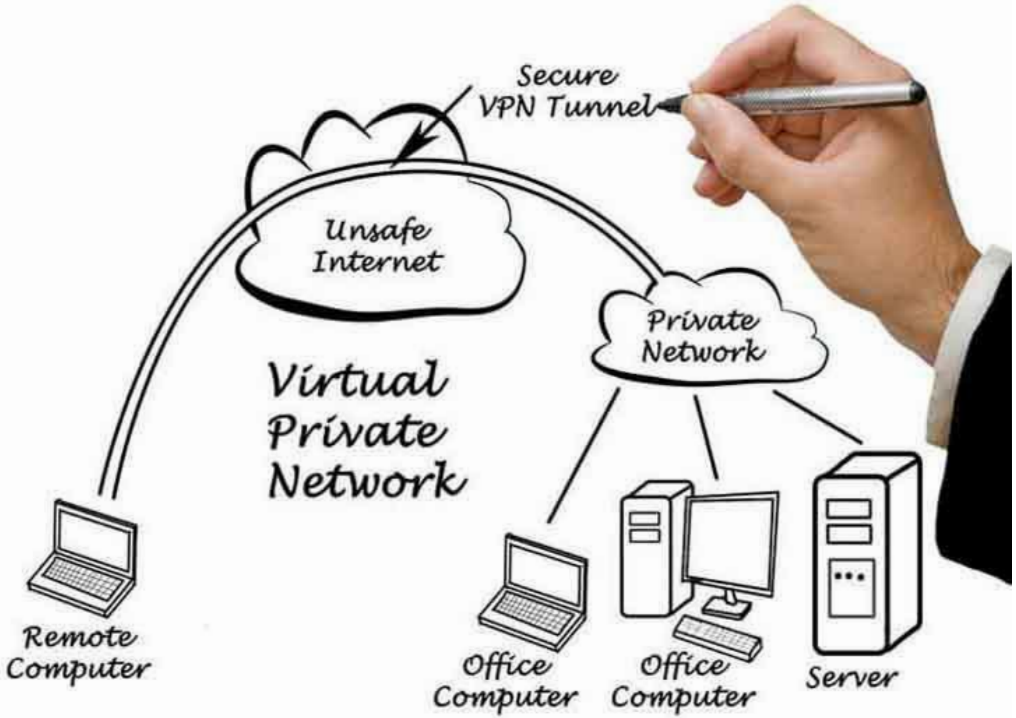
Nihov širok spektar uredjaja ga svrstava u odnos cena-kvalitet na najvišem njivou
https://mikrotik.com/products

VPN – METODE TOPOLOGIJA

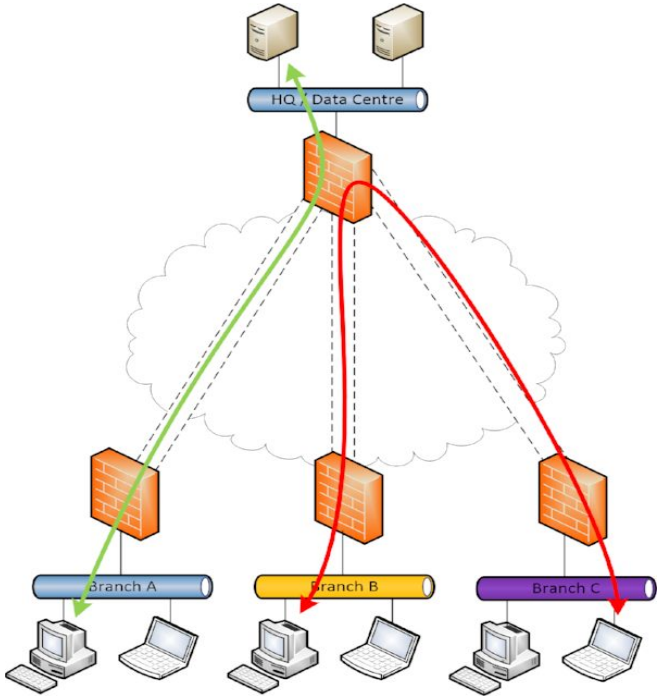
-Hub and Spoke
-Site to Site
-Full Mesh

-Clent to server

-Hybrid – Partial mesh



Hub and Spoke

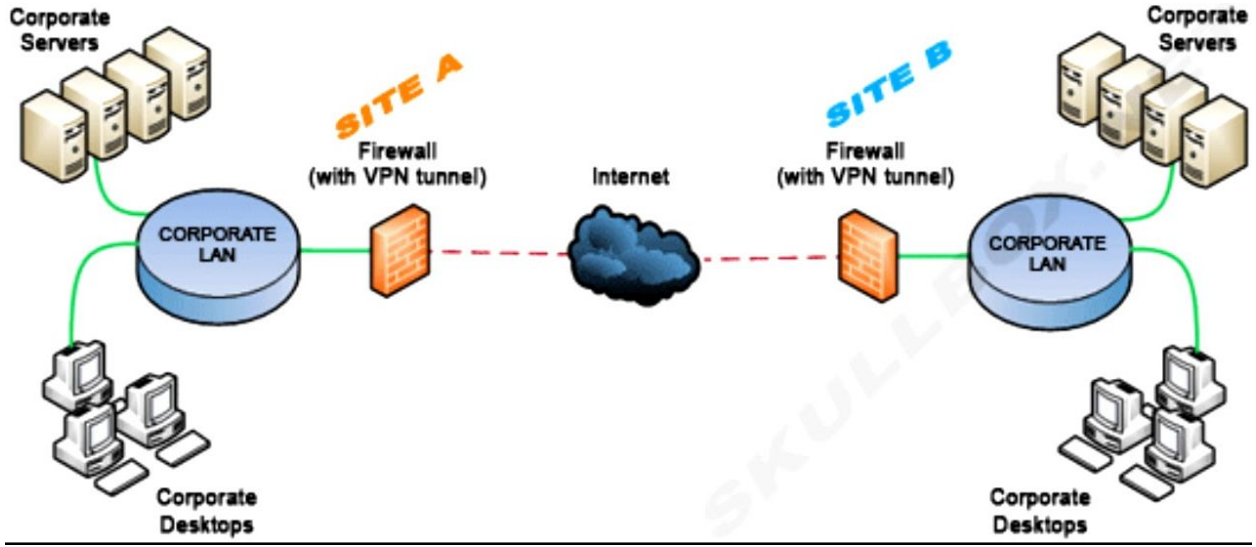


Hub and Spoke

- Poznata još i kao site to multi-site VPN
- Sve lokacije su povezane sa HQ(centralnom) lokaciom
- Lokacije komuniciraju sa ostalim lokacijama preko HQ lokacije
- HQ lokacija vrši kontrolu saobraćaja
- Dosta je primenjiva i rasprostanjena vrsta topologije

- Mora se voditi racuna o redudantnosti
- Sporija komunikacija izmedju lokacija

Site to Site


Corporate Servers
SITE A
Firewall (with VPN tunnel)
Internet
SITE B
Firewall (with VPN tunnel)
Corporate Servers
CORPORATE LAN
CORPORATE LAN
Corporate Desktops
Corporate Desktops

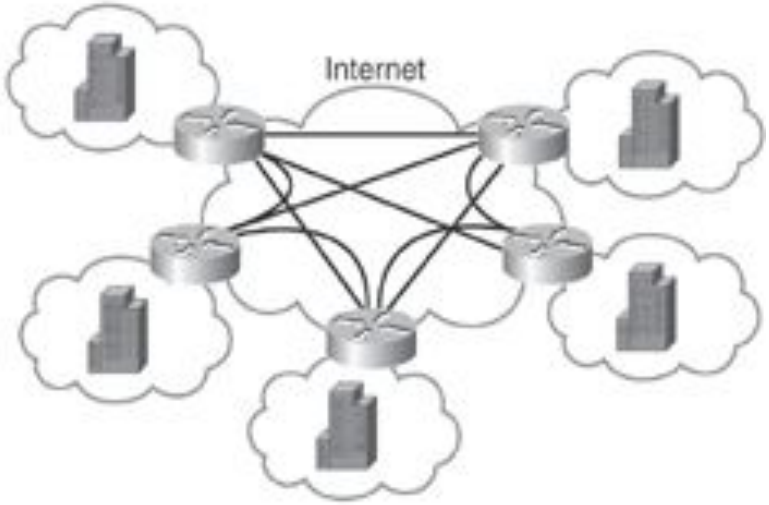
Site to Site

- VPN izmedju dve lokacije

- Omogućava deljenje podataka

- Koristi se sigurni VPN tuneli radi zaštite podataka

Full Mesh

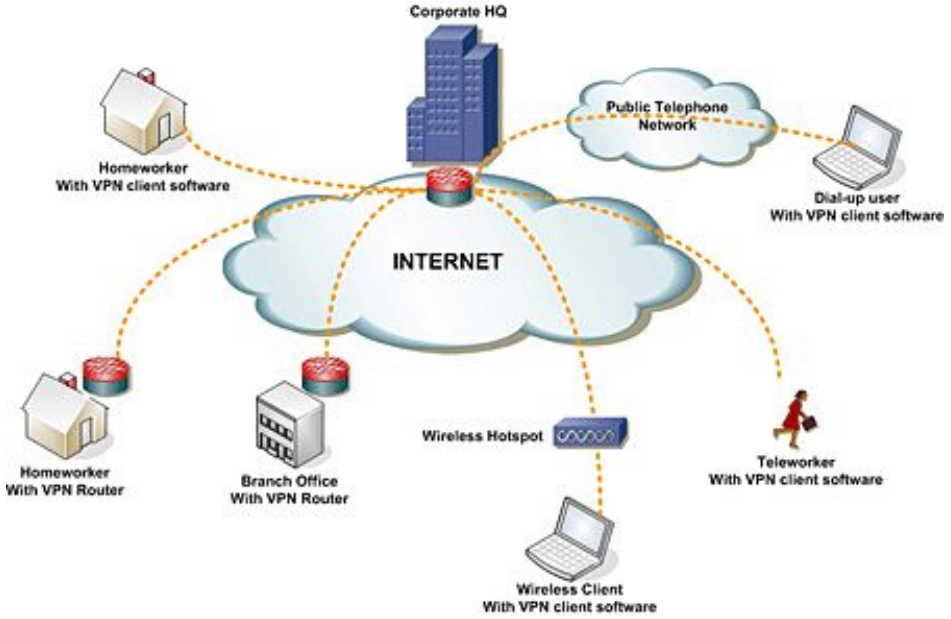


Full Mesh

- VPN svako sa svakim
- Sve lokacije komuniciraju medjusobno
- Brza , stabilna i redudanta VPN konekcija

- Teže sa konfiguraciju i održavanje
- Više hardwerskih resursa

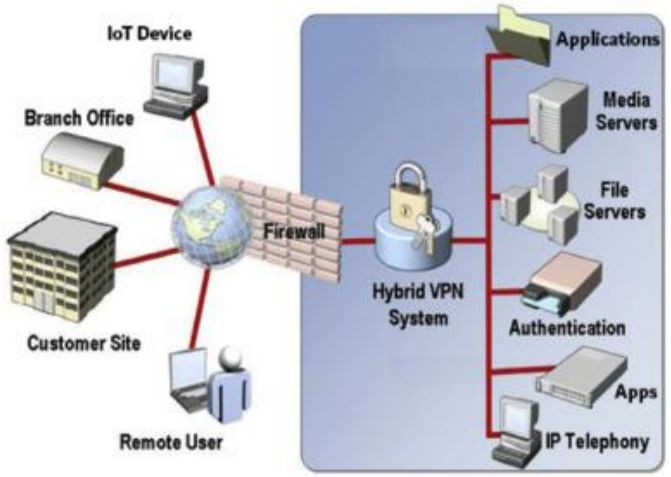
Client to server VPN

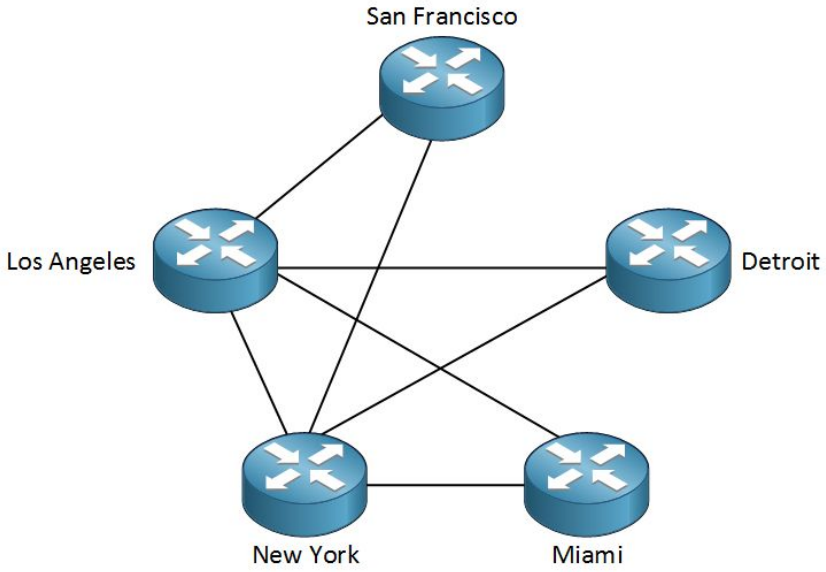


Client to server VPN

- Najviše se koristi kada je reč o kućnim korisnicima
- Omogućava pristup sa bilo koje tačke u svetu
- Podržavaju svi tipovi operativnih sistema
- Postoje slučajevi gde se instalira softver
- Podržava veliki broj prozvođača opreme

Hybrid – Parital mesh VPN





Hybrid – Partial mesh VPN

- Koriste više vrsta VPN tunela za komunikaciju

- Može se kombinovati više topologija

- Pružaju redudantnost

- Teže sa konfiguraciju i održavanje

MIKROTIK – VPN TUNELI

- Mikrotik oprema podržava veliki broj VPN tunela i od zavisnosti od modela topologije može se primeniti u raznim sverama modernog biznisa .

- Prednost MT uredjaja jeste jednostavnost konfiguracije

- Može da radi i kao klijent i kao server

- Može raditi sa ostalim vendorima

MIKROTIK – TIPOVI VPN TUNELA

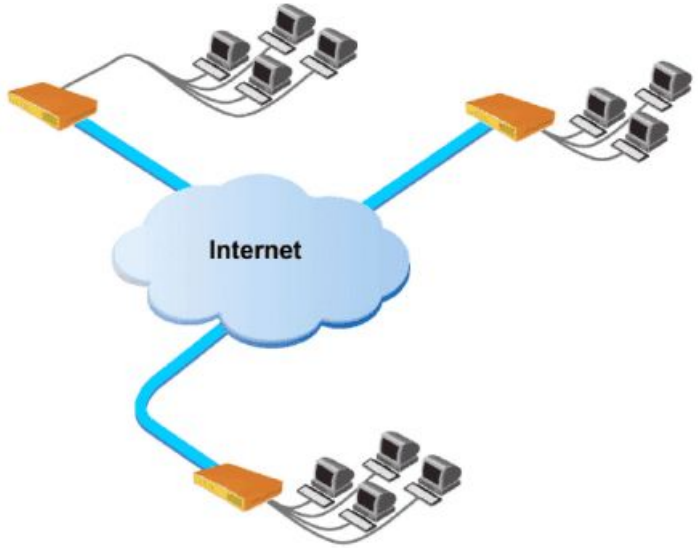
GRE – IPIP tunell

EoIP
MPLS-VPLS

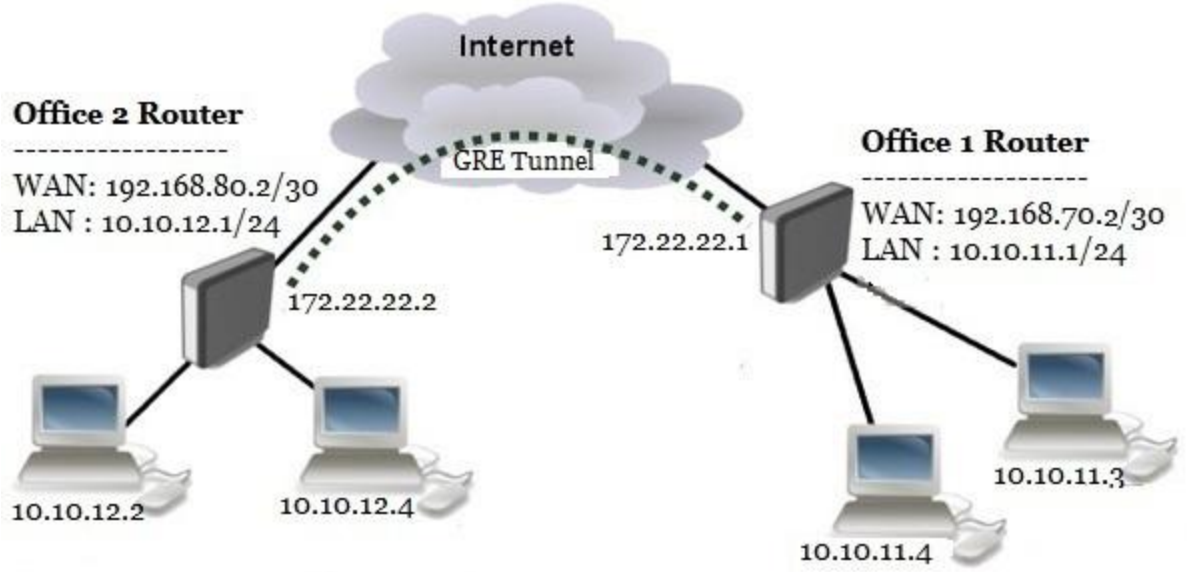
IPSec tunell

L2TP – PpTP

OVPN - SSTP



GRE – IPIP tunell
(Generic Routing Encapsulation protocol)



GRE – IPIP tunell

- GRE je protkol koji je prvobitno razvio Cisco

- GRE tuneli vrše enkapsulaciju I mogu da transportuju druge protokole kroz mrežu

- GRE protokol se koristi kod mnogih tipova VPNa

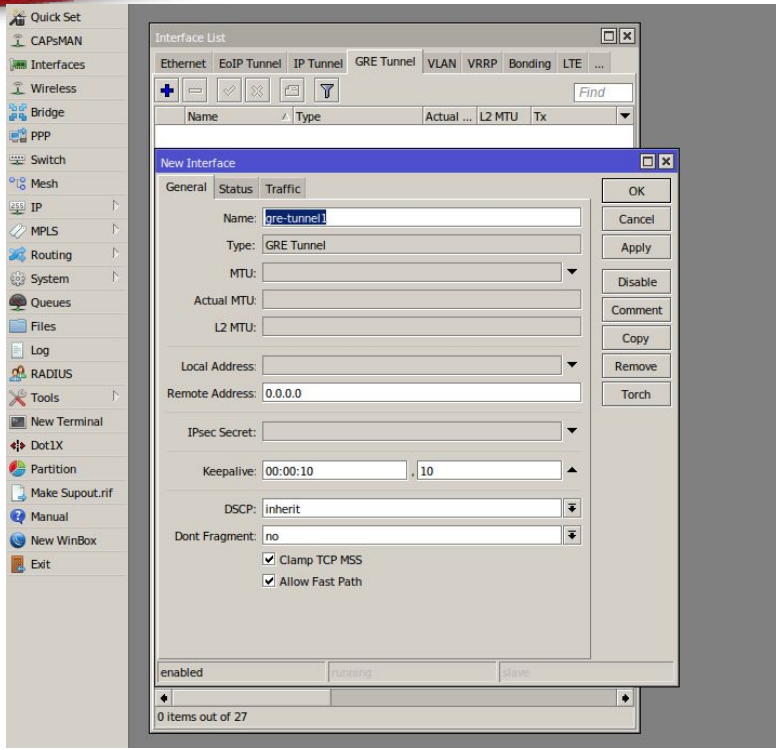
GRE – IPIP tunell

- IPIP tunlel sa druge strane radi kao I sto je napisano : jedan IP paket u drugom

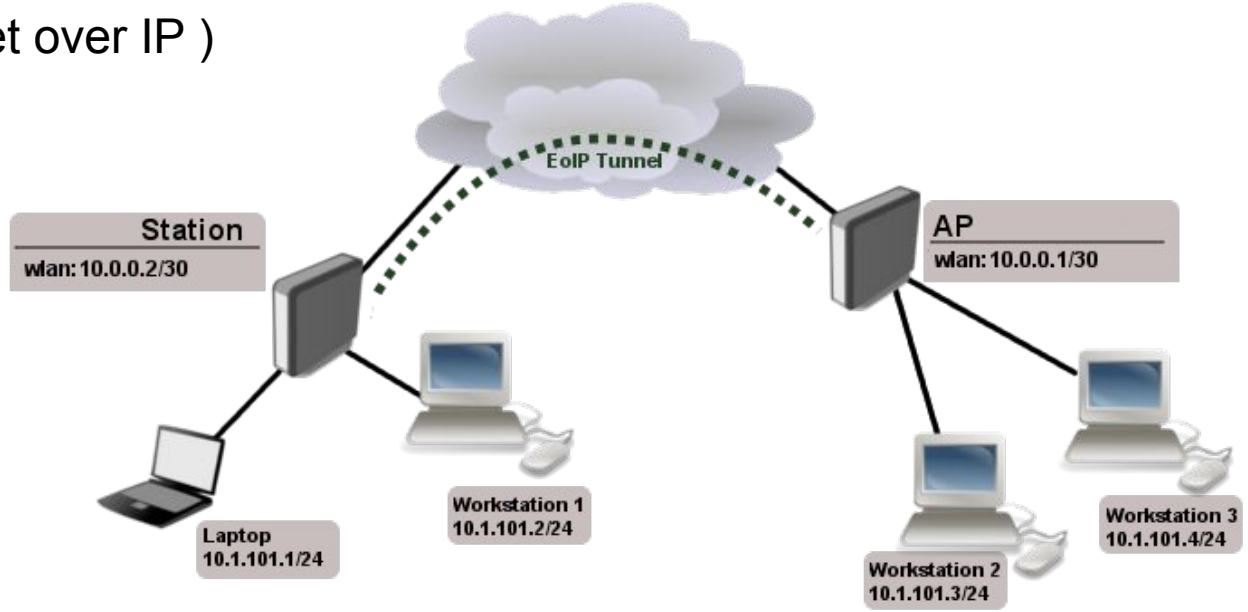
- IPIP ne može da prenosi druge protokole , multikast I IPv6 saobraćaj

- Oba protokola su opšte korićena i podržana
- Zbog enkapsulacije GRE je sigurniji tunel ali je I dalje NESIGURAN

GRE – IPIP tunell



EoIP tuneli (Ethernet over IP)



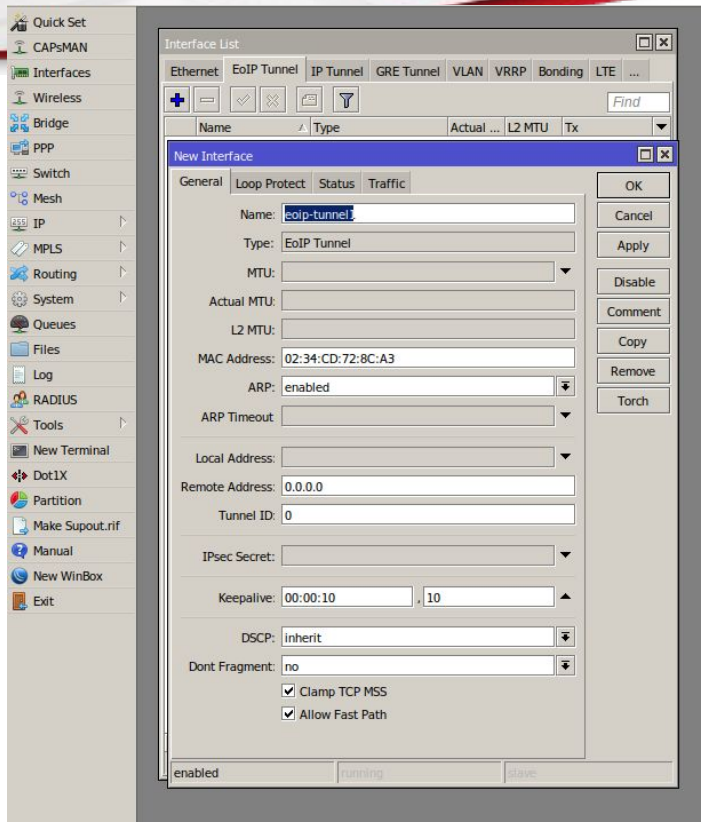
EoIP tuneli

- Mikrotik protokol

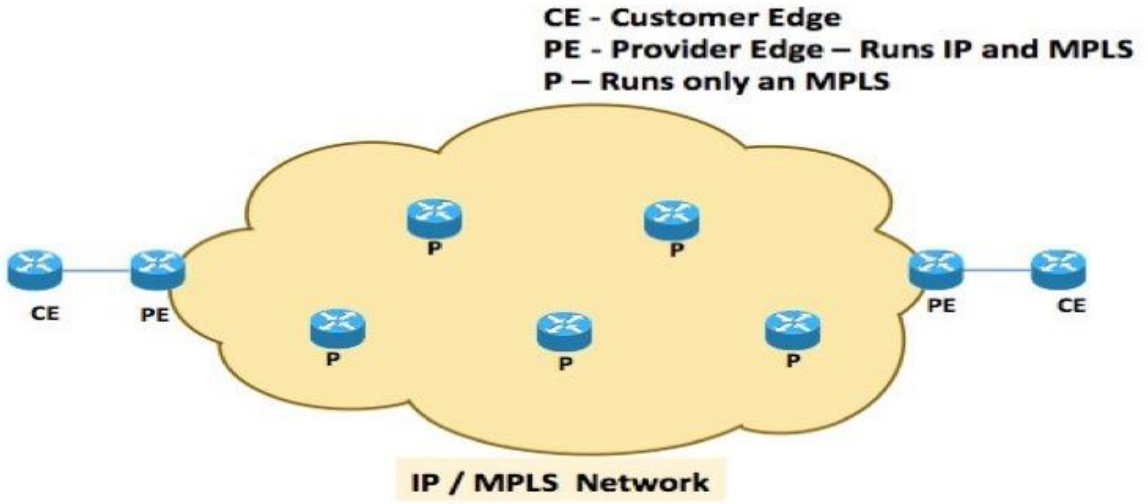
- Koristi GRE za enkapsulaciju tako da može da prenese nonIP protokol
- Može biti L2 I L3
- Kada se koristi kao L2 transportuje broadcast
- Koristi tunel ID za identifikaciju tunela koji mora da bude identičan sa obe strane

- Nije zaštićen protokol

EoIP tuneli


Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
Partition
Make Supout.rif
Manual
New WinBox
Exit
Interface List
Ethernet
EoIP Tunnel
IP Tunnel
GRE Tunnel
VLAN
VRRP
Bonding
LTE
Find
Name
Type
Actual ...
L2 MTU
Tx
New Interface
General
Loop Protect
Status
Traffic
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch
Name: eoip-tunnel1
Type: EoIP Tunnel
MTU:
Actual MTU:
L2 MTU:
MAC Address: 02:34:CD:72:8C:A3
ARP: enabled
ARP Timeout
Local Address:
Remote Address: 0.0.0.0
Tunnel ID: 0
IPsec Secret:
Keepalive: 00:00:10 , 10
DSCP: inherit
Dont Fragment: no
Clamp TCP MSS
Allow Fast Path
enabled
running
slave

MPLS-VPLS tuneli
(Multi Protocol Label Switching – Virtual private LAN servis)



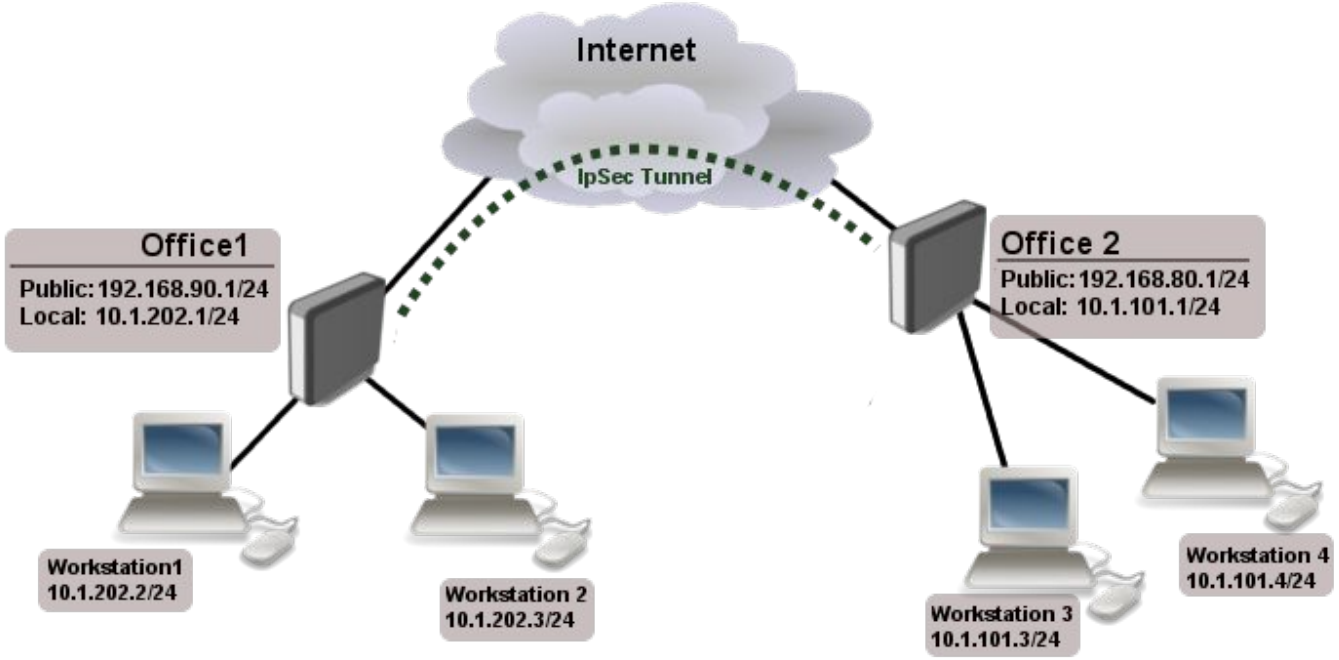
MPLS-VPLS tuneli

- Protokol ISP (internet servis provajdera)

- Inportuje labele tako da je brži od rutiranja
- Vrši enkapsulaciju u MPLS I može da transportuje veliki broj NonIP protokola
- Može da bude L2 i L3
- Mora se prvo konfigurisati MPLS da bi VPLS bio aktivan

- Koristi puno memoriskih resursa
- Svi ruteri moraju da podržavaju MPLS protokol

IPSec tuneli



IPsec tuneli

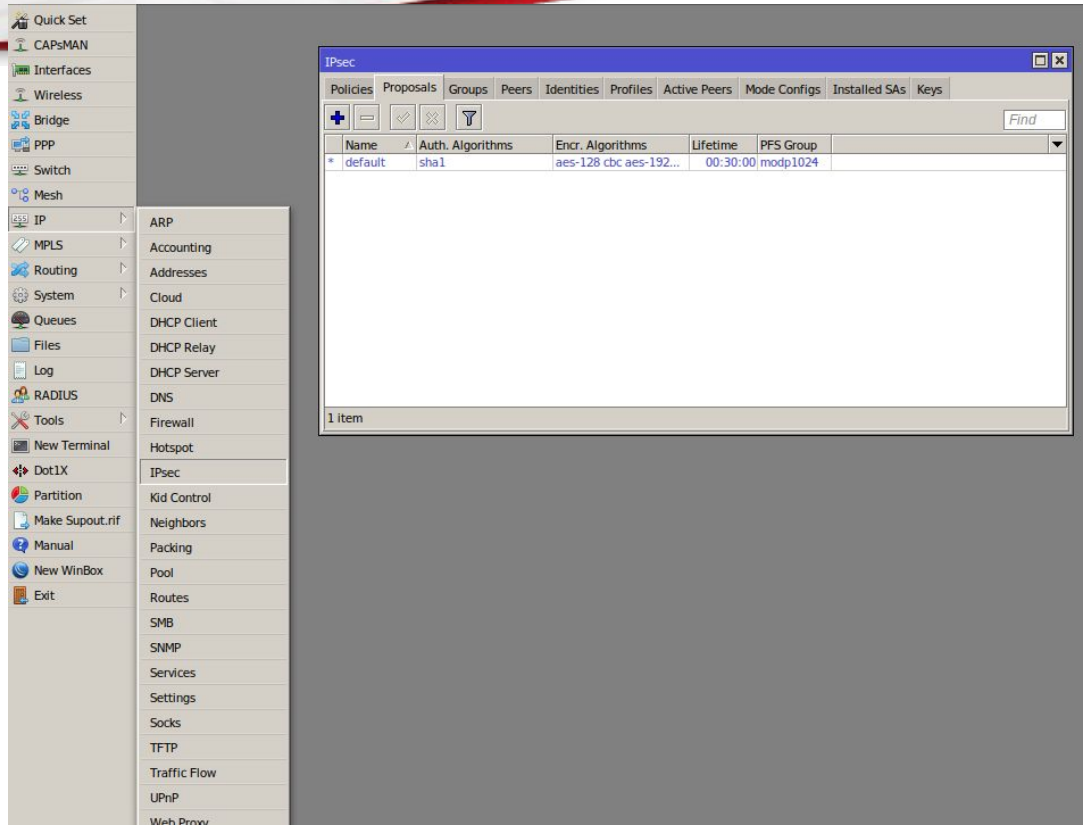
- IP Security protokol je jedan od nasigurnijih protokola današnjice

- Koristi enkripciju i autentifikaciju kao i razne metode zaštite kako bi osigurao vezu
- Praktično je nemoguće hakovati tunel
- Može se birati jačina enkripcije

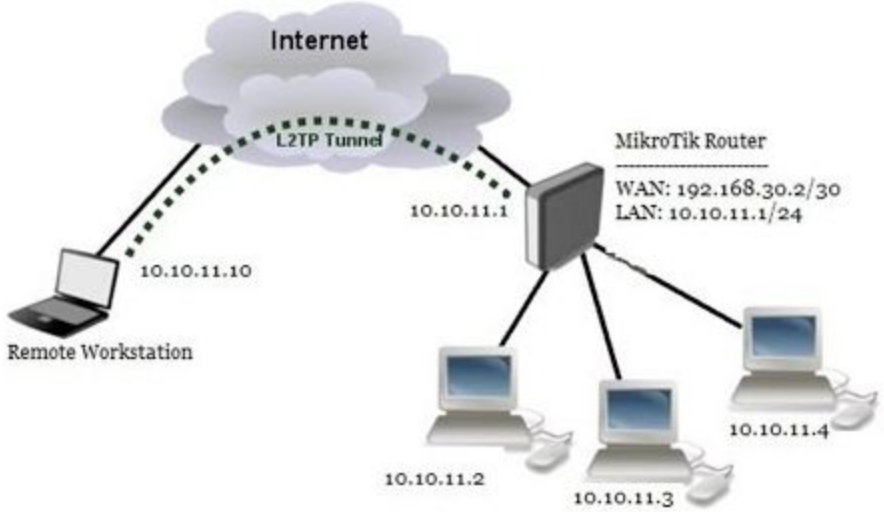
- Može da radi u konbinaciji sa drugim protokolima

- Jača enkripcija znači više resursa i jači ruter
- Komplikovan za konfiguraciju

IPsec tuneli



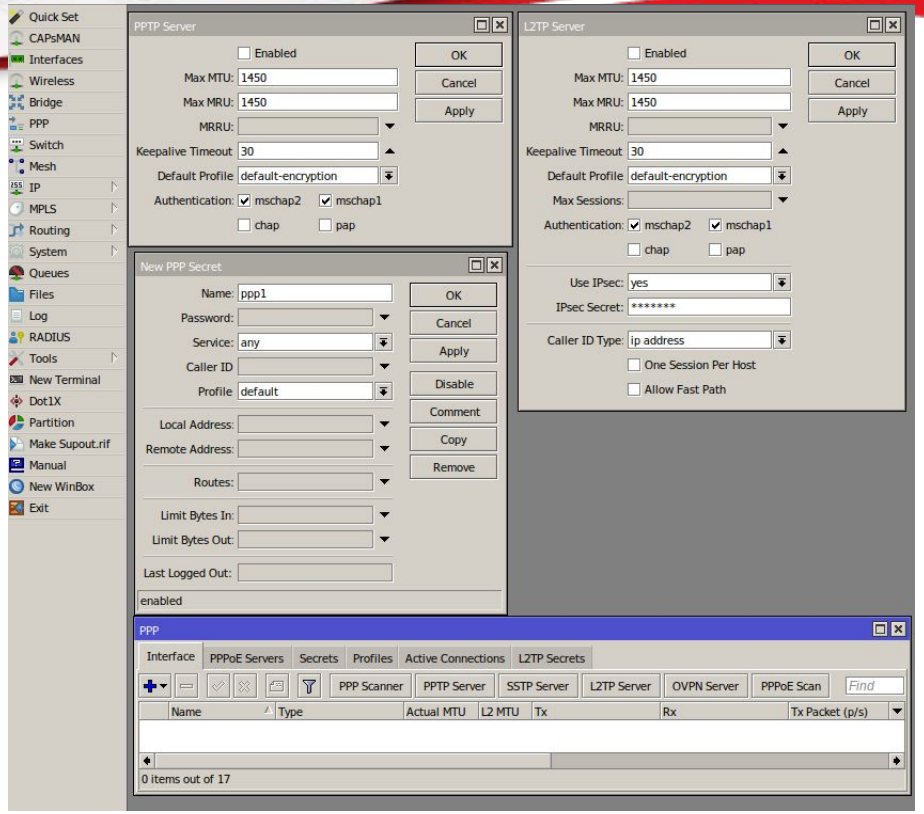
PPtP-L2TP tuneli
(Point to point tuneling protocol – Layer 2 tunelling protocol)



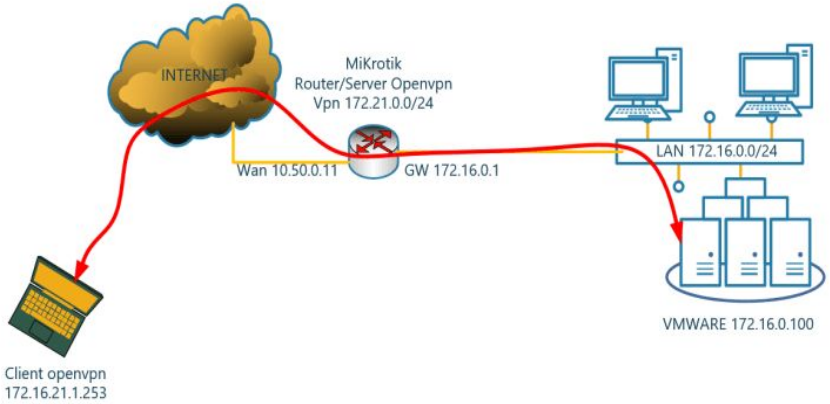
PPtP-L2TP tuneli

- PPtP protokol je prvobitno razvio Microsoft radi povezivanja udaljenih korisnika na komporativnu mrežu preko bilo koje ISP tehnologije
- Vrši enkripciju i autenifikaciju
- Koristi GRE za prenos podataka i može se koristiti na skoro svm vrstama OS-a (Microsoft , MAC , Linux , Android …)
-L2TP su razvijali Microsoft I Cisco I služi kao I PptP za povezivanje na korporativnu mrežu kroz bilo koju vrsti ISP tehnologije
- Često se koristi sa IPSecom
- PPTP je laksi za setup i brzi je ali je manje siguran od L2TP koji je malo sporiji ali sa kombinacijom IPSec-a je mnogo više sigurniji
- Oba protokola korise remote ID username i pasword za povezivanje

PPtP-L2TP tuneli



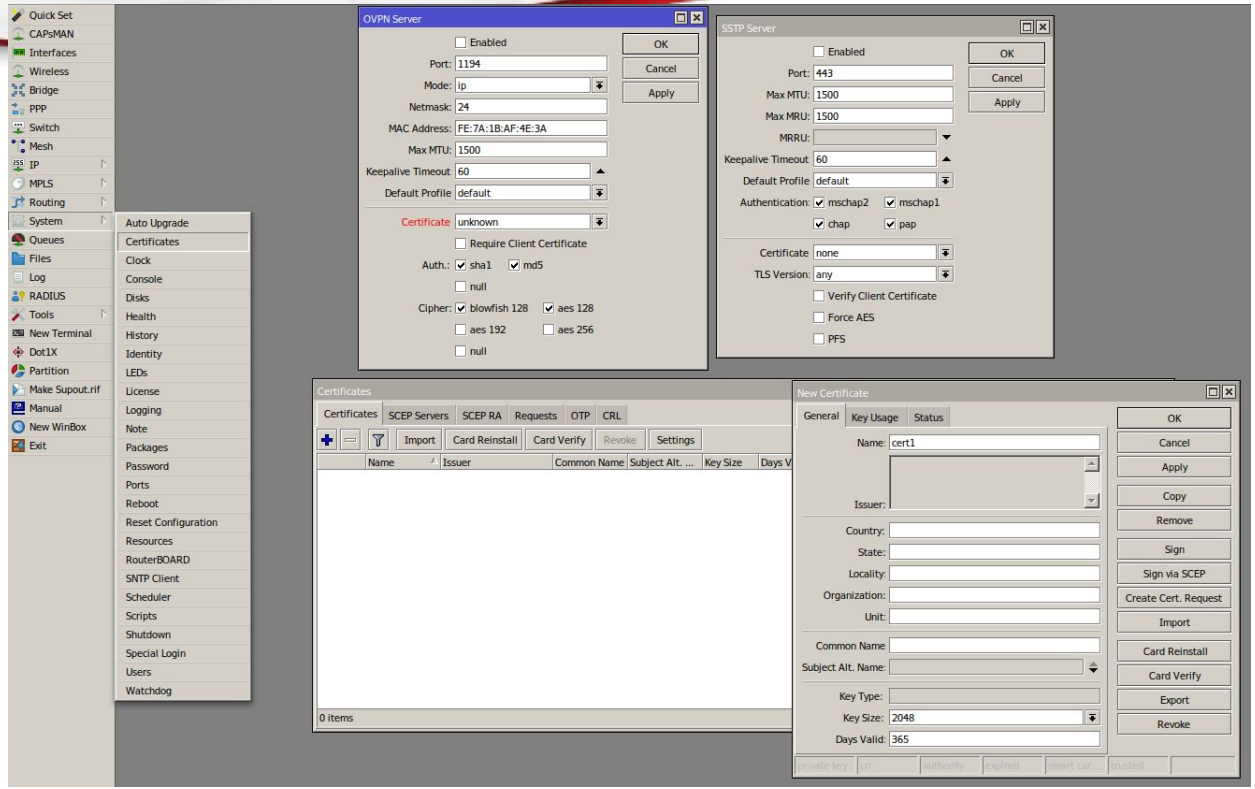
OVPN – SSTP – (SSL)
(Open VPN – Secure socket tunneling protocol (Secure sockets layer))

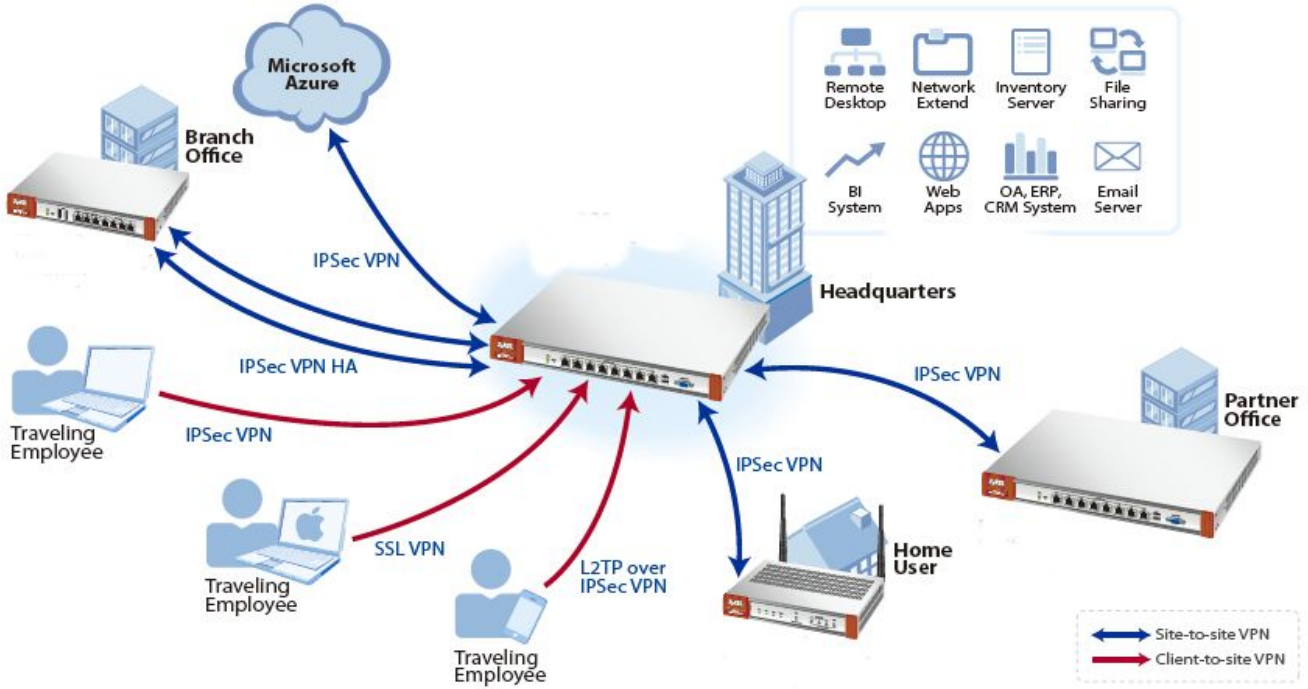


- OVPN protokol koristi SSL (secure sockets layer) vrstu bezbednosti koja slicna Ipsec služi za zaštitu izmedju konekcija
- Može da radi iza NAT-a , koristi TCP I UDP za uspostavu konekcija
- Za razliku od ostalih ovo je open-source protokol , ali mora da se instalira kao softver

- SSTP je razvio Microsoft i isto koristi SSL ako i OVPN
- Može da radi iza NAT-a ali koristi TCP za uspostavu konekcija
- Nativno ide sa Windows OS (WIN 7)

- Mikrotik ima mogucnost da kreira svoj SSL sertifikat


Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
Partition
Make Supout.rif
Manual
New WinBox
Exit
Auto Upgrade
Certificates
Clock
Console
Disks
Health
History
Identity
LEDs
License
Logging
Note
Packages
Password
Ports
Reboot
Reset Configuration
Resources
RouterBOARD
SNTP Client
Scheduler
Scripts
Shutdown
Special Login
Users
Watchdog
OVPN Server
Enabled
Port: 1194
Mode: ip
Netmask: 24
MAC Address: FE:7A:1B:AF:4E:3A
Max MTU: 1500
Keepalive Timeout: 60
Default Profile: default
Certificate: unknown
Require Client Certificate
Auth.: sha1 md5
null
Cipher: blowfish 128 aes 128
aes 192 aes 256
null
OK
Cancel
Apply
SSTP Server
Enabled
Port: 443
Max MTU: 1500
Max MRU: 1500
MRRU:
Keepalive Timeout: 60
Default Profile: default
Authentication: mschap2 mschap1
chap pap
Certificate: none
TLS Version: any
Verify Client Certificate
Force AES
PFS
OK
Cancel
Apply
Certificates
Certificates SCEP Servers SCEP RA Requests OTP CRL
Import Card Reinstall Card Verify Revoke Settings
Name Issuer Common Name Subject Alt. ... Key Size Days V
0 items
New Certificate
General Key Usage Status
Name: cert1
Issuer:
Country:
State:
Locality:
Organization:
Unit:
Common Name:
Subject Alt. Name:
Key Type:
Key Size: 2048
Days Valid: 365
OK
Cancel
Apply
Copy
Remove
Sign
Sign via SCEP
Create Cert. Request
Import
Card Reinstall
Card Verify
Export
Revoke
private key
ca
authority
expired
smart card
trusted


Microsoft Azure
Branch Office
IPSec VPN
IPSec VPN HA
Traveling Employee
IPSec VPN
Traveling Employee
SSL VPN
Traveling Employee
L2TP over IPSec VPN
Headquarters
Remote Desktop
Network Extend
Inventory Server
File Sharing
BI System
Web Apps
OA, ERP, CRM System
Email Server
IPSec VPN
Partner Office
IPSec VPN
Home User
Site-to-site VPN
Client-to-site VPN

ŠTA IZABRATI !!!!

Hub and spok -Full Mesh – GRE – IPIP – Ipsec
Site to Site – IP sec
Client Server – SSTP,OVPN,L2TP with IP sec , PptP)

- Izabrati kvalitetan hardwer posebno za centralnu lokaciju

- Koristiti što sigurniju metodu povezivanja

- Dizajn je Veoma vazan

Hvala :)

https://www.linkedin.com/in/zoranantoncic/