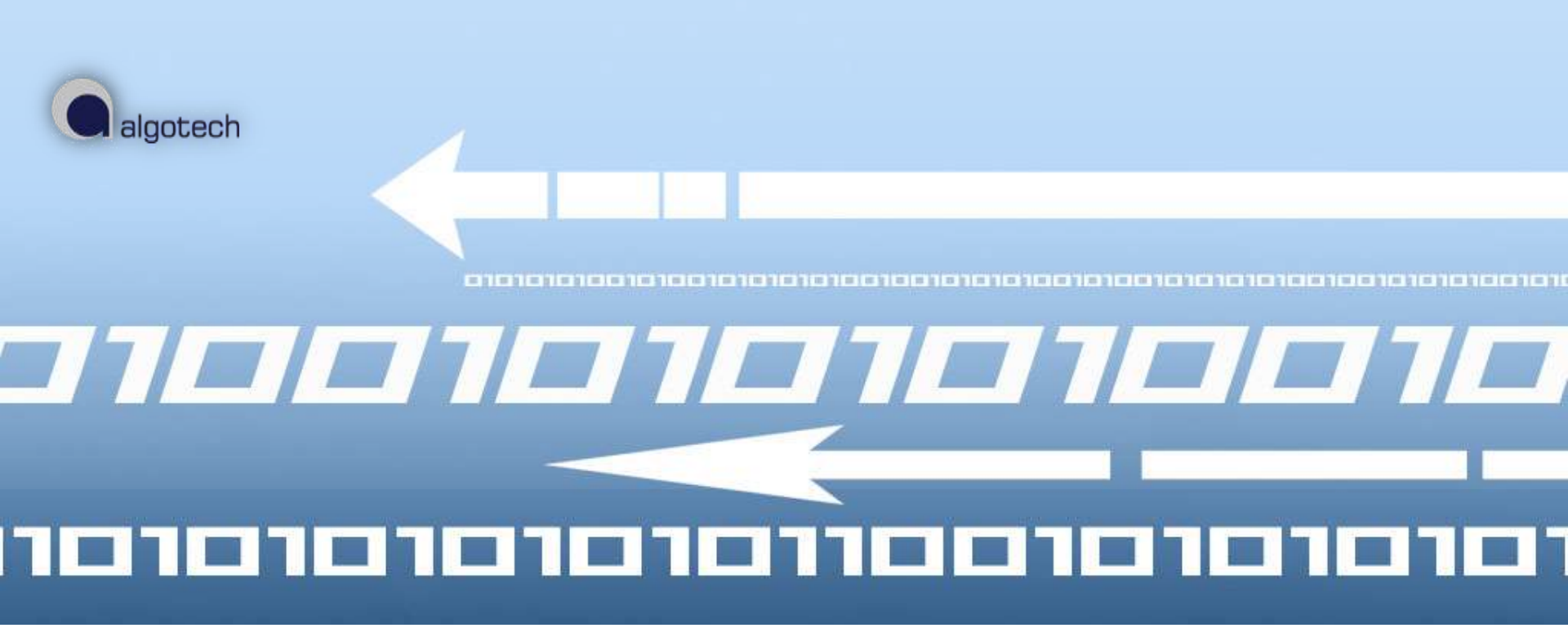


Mikrotik IPSec servisi

MUM Beograd, Srbija
10.10.2016.

Srđan Stanišić

verzija 1.0 rs

Autor i njegova interesovanja

- IT/IS Manager u Algotech d.o.o.
- U IT industriji od 1991. godine
- Usmerenje ka Windows poslovnim mrežama i bezbednosti informacija
- Sertifikati za Microsoft, CompTIA, NICE
- Autor dve knjige o mrežama
- Sa Mikrotik ruterima radi od 2005. godine
- Fokus na kontroli pristupa i automatizaciji rada

Agenda

- Šta je to IPSec?
- Povezivanje dve Internet lokacije preko IPSec tunela
- Zaštita drugih tipova tunela IPSec-om
- L2TP/IPSec za udaljene korisnike („roadwarrior“ režim)
- Demonstracija u virtuelnom okruženju

Šta je to IPSec?

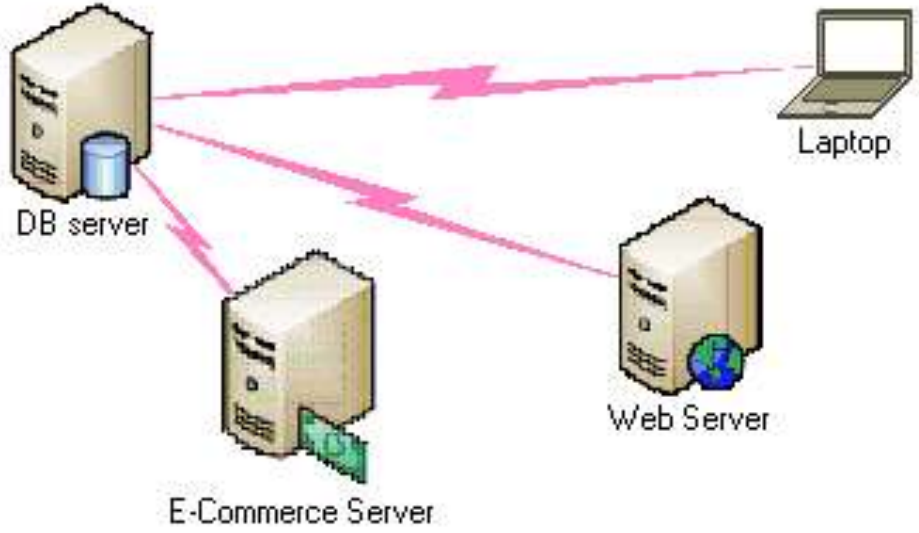
- IPSec je skup servisa koji omogućavaju razmenu podataka u zaštićenom obliku preko nezaštićenih IPv4 ili IPv6 mreža
- IPSec tunel je nerutabilni dinamički tunel između dve tačke u mreži
- Današnji de facto standard za sigurnu Internet komunikaciju

IPSec protokoli

- IPSec familija se sastoji iz sledećih protokola:
  - Authentication Header (AH) – RFC 4302
  - Encapsulating Security Payload (ESP) – RFC 4303
  - Internet Key Exchange (IKE)
- Možemo koristiti samo AH, samo ESP ili AH i ESP
- IPSec protokoli su izuzetno osetljivi na vremensku sinhronizaciju – NTP protokol mora da se koristi na oba uređaja!

Režimi rada

- **Transport** režim štiti saobraćaj između dva direktno povezana hosta



- **Tunnel** režim služi za zaštitu saobraćaja između dve mreže ili dva hosta koji komuniciraju kroz gejtveje

Authentication Header (AH)

- AH protokol je namenjen za zaštitu autentičnosti sadržaja, ali ne i za njegovo šifrovanje.
- Vrednost AH će zavisiti od sadržaja podataka unutar paketa
- Pozicija dodatnog zaglavlja zavisi od režima tunela koji se koristi
- Za proveru identiteta (*authentication*) se koriste algoritmi
  - MD5
  - SHA1

Encapsulating Security Payload (ESP)

- ESP protokol se koristi za zaštitu sadržaja paketa.
- Koristi svoju proveru identiteta i ne zahteva AH.
- Upotreba AH ojačava zaštitu paketa
- Za šifrovanje podataka se koristi neki od poznatih algoritama:
  - DES
  - 3DES
  - AES 128/192/256-bita
  - Blowfish
  - Camellia 128/192/256-bita
  - Twofish

Hardversko šifrovanje ESP protokola

- Na jačim modelima Mikrotik Routerboard-ova je podržano je hardversko šifrovanje ESP protokola
  - RB 1000
  - RB 1100AHx2
  - Svi Cloud Core Router (CCR) uređaji
  - RB 850Gx2
- CPU je optimizovan za bržu obradu AES-CBC i SHA1/SHA256 algoritama, sve ostalo se radi softverski

Internet Key Exchange protokol

- IKE je najzastupljeniji protokol za razmenu ključeva preko Interneta
- IKE daemon se aktivira kada treba uspostaviti razmenu ključeva, obezbediti međusobnu proveru identiteta dva hosta i započeti upravljanje *security associations* (SA) identifikatorima
- IKE ima dve faze uspostavljanja komunikacije:
  - IKE I
  - IKE II

IKE I faza

- Kada se uoči potreba za formiranjem tunela, uređaji (najčešće 2 rutera) započinju međusobno povezivanje
- Da bi se tunel uspostavio, oba uređaja moraju da imaju definisanog partnera (**Peer**)
- Treba da znamo sledeće parametre:
  - IP adresu druge strane
  - Algoritam za proveru identiteta (MD5, **SHA-1**…)
  - Algoritam za šifrovanje saobraćaja (3DES, **AES**…)
  - Vreme važenja ključa
  - Diffie-Helman (DH) grupu (minimalno DH2 – 1024 bita)
  - Da li ćemo komunicirati kroz NAT (NAT-T opcija)
  - DPD podešavanja
  - Vreme života tunela (npr. 1 dan)

Diffie-Helman algoritam

- Diffie-Helman (DH) algoritam je osmišljen sa ciljem da dve strane, koje nemaju zajednički deljeni ključ za šifrovanje, mogu da ga naprave u bilo kom trenutku
- Stvoren je za pravljenje dinamičkih ključeva preko Interneta
- Ovako napravljen ključ će šifrovati sav ostali saobraćaj
- Opisan u RFC 2409 i RFC 3526
- Minimalno treba koristiti ključ od 1024 bita i to je DH group 2
- Preporuka je da se koriste jači ključevi

IKE II faza

- Kada se uspešno završi faza I, imamo dinamički napravljene ključeve koji će se koristiti za dalje operacije
- Da bi se ova faza uspostavila, moramo da imamo:
  - pravila za komunikaciju (**policies**) i
  - skup pravila za zaštitu (**proposal**)
- Pravila moraju da budu identična na obe strane
- Treba usaglasiti:
  - IPSec protokol (AH, ESP, AH i ESP)
  - Režim rada (tunel ili transport)
  - Vreme života (lifetime) – npr. 30 minuta
  - PFS grupu (takođe DH ključ)

Perfect Forward Secrecy (PFS)

- PFS je mehanizam koji menja ključ za šifrovanje saobraćaja na kraćem intervalu od života celog tunela
- Koristi se isti algoritam kao i kod uspostavljanja tunela u fazi I
- Ideja je da se omogući dodatna zaštita razmenjenog sadržaja u toku života IPSec tunela
- PFS dodatno opterećuje procesor za izračunavanje ovih ključeva
- Koristiti minimum DH grupu 2

Život tunela

- Svi tuneli se prave sa ograničenim vekom trajanja
- Svaki novi tunel je šifrovan drugim ključem
- Životni vek se ograničava
  - Vremenski
  - Na količinu podataka
- Za svako ograničenje postoje dva brojača:
  - Meki (soft)
  - Čvrsti (hard)
- Meki brojač se koristi da se odredi vreme obnavljanja tunela.
- Čvrsti brojač se koristi da se odredi vreme kada se tunel ukida.

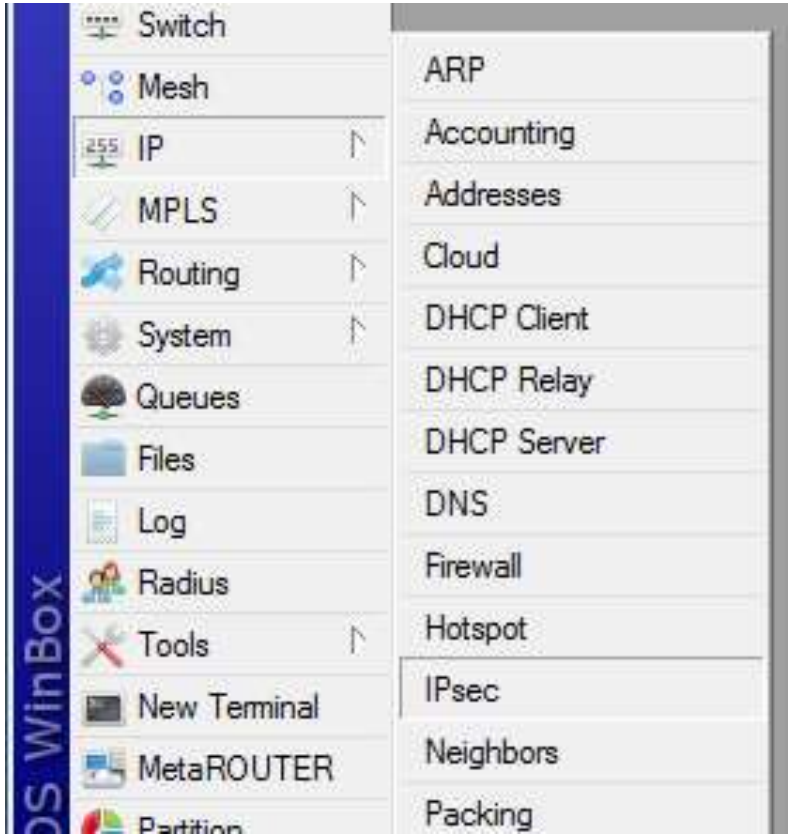
Neophodna licenca za IPSec

- Detaljan opis nivoa licenciranja je naveden na stranici: http://wiki.mikrotik.com/wiki/Manual:License

Nivo (level)	*Broj IPSec tunela*
0 (24h trial)	*Bez ograničenja*
1 (free demo)	*Nije navedeno*
3 (CPE)	*Nije navedeno*
4	*Nije navedeno*
5	*Nije navedeno*
6	*Bez ograničenja*

Gde se nalaze IPSec servisi?

- IPSec servise nalazimo u meniju IP > IPSec ili u `/ip ipsec` u konzoli
- Instaliran je na svakom Routerboard-u
- Na x86 platformi treba da se instalira **security** paket
- Paket **ppp** daje podršku samo za PPP, PPTP, L2TP, PPPoE i ISDN PPP servise



FT1P ☺ - jedan važan dokument

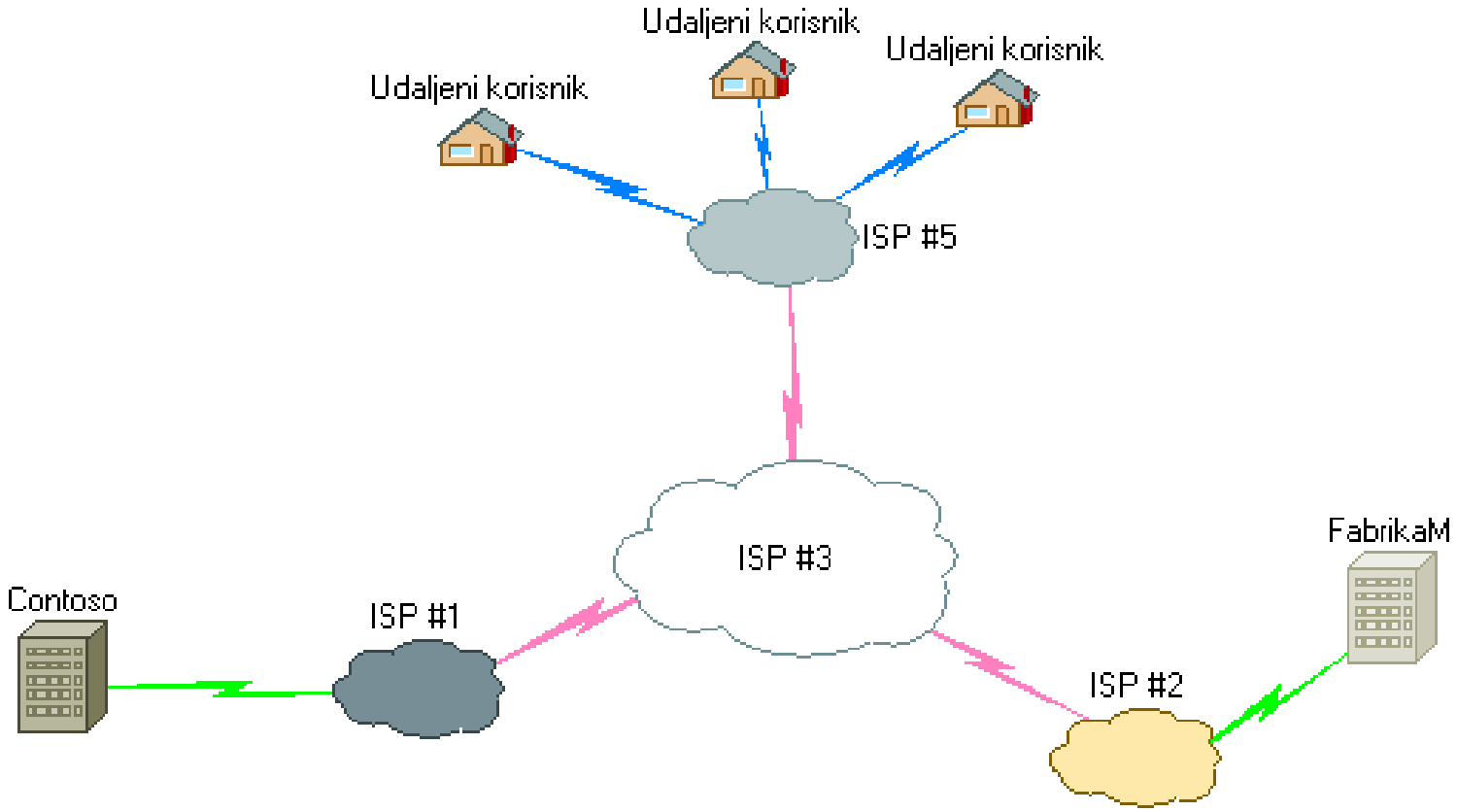
- Napravite dokument sa svim parametrima pre konfiguracije

Страна	Contoso	Fabrikam
Уређај	Mikrotik x86 v6.33	Mikrotik x86 v4.17
Јавна адреса	203.0.113.17	203.0.113.29
IKE Phase I (IPSec Peer)		
Authentication method	Preshared key	Preshared key
Secret	Биће размењен СМСом (Test1234)	
Exchange Mode	Main	
Proposal Check	Obey	
Hash Algorithm	SHA1	SHA1
Encryption Algorithm	AES256	AES256
DH Group	DH group2/modp1024	DH group2/modp1024
Lifetime	1d 00:00:00 (86400 seconds)	1d 00:00:00 (86400 seconds)
DPD Interval	120 s	120 s
DPD Maximum Failures	5	5
IKE Phase II (IPSec Proposal)		
Auth Algorithm	SHA1	SHA1
Encryption Algorithm	AES256	AES256
Lifetime	00:30:00 (1800 seconds)	00:30:00 (1800 seconds)
PFS Group	DH group2/modp1024	DH group2/modp1024
Интересантан саобраћај (полисе)		
Сервер/опсег	WWW 198.51.100.10 mail 198.51.100.11	192.0.2.0/24
Порт(ови)	sve	sve
Протоколи	esp	esp

Naša laboratorija – praktični primeri

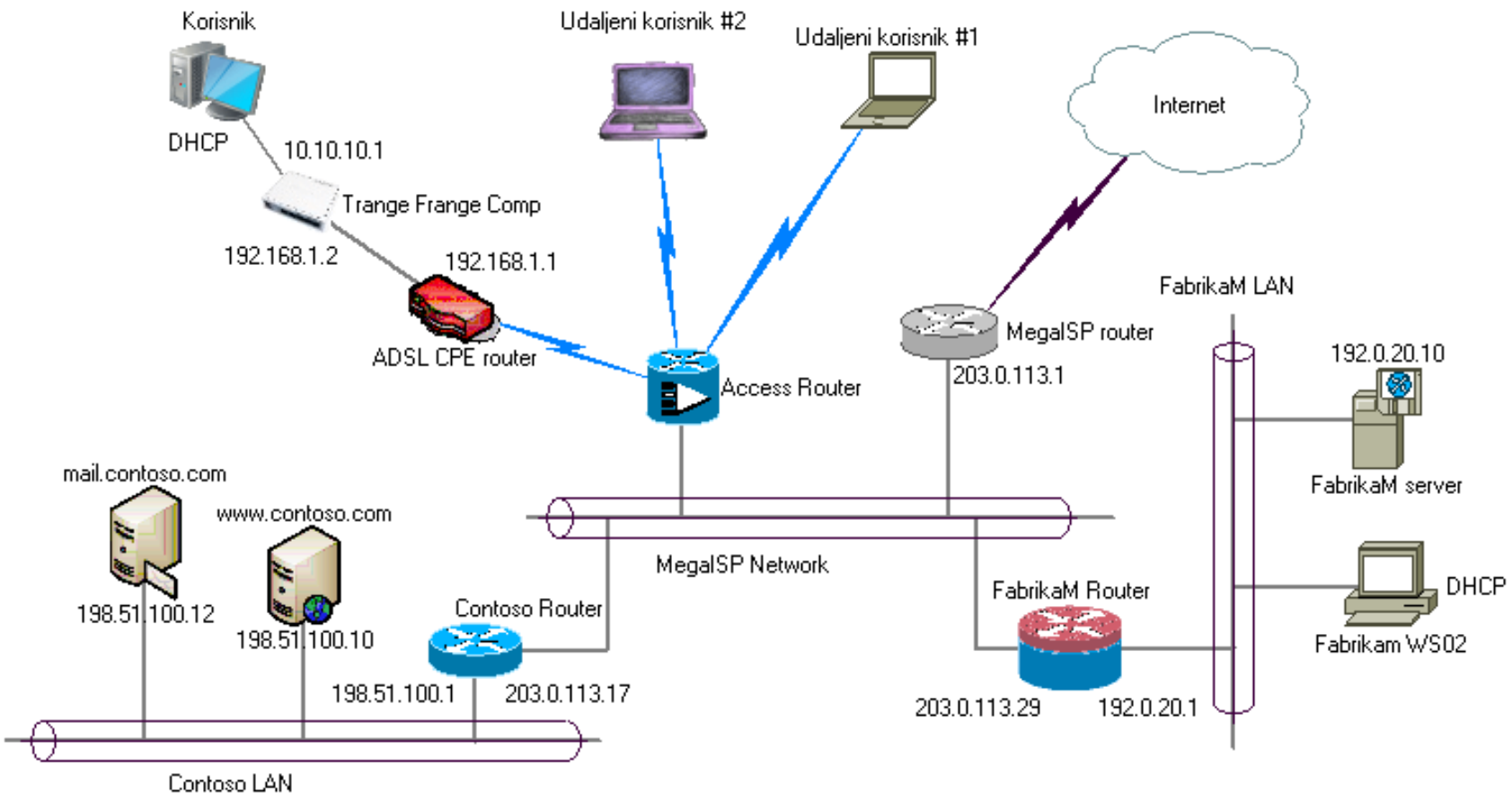
Scenario koji simuliramo

- Simulirali smo povezivanje više organizacija, ISP-ova i udaljenih pojedinačnih korisnika



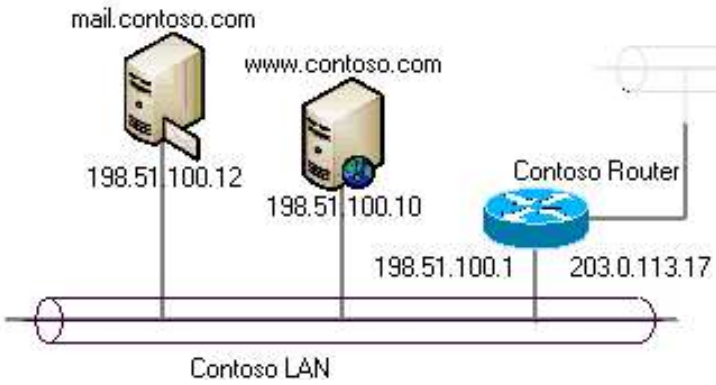
Virtuelno okruženje

- Sve funkcije smo simulirali u virtuelnom okruženju



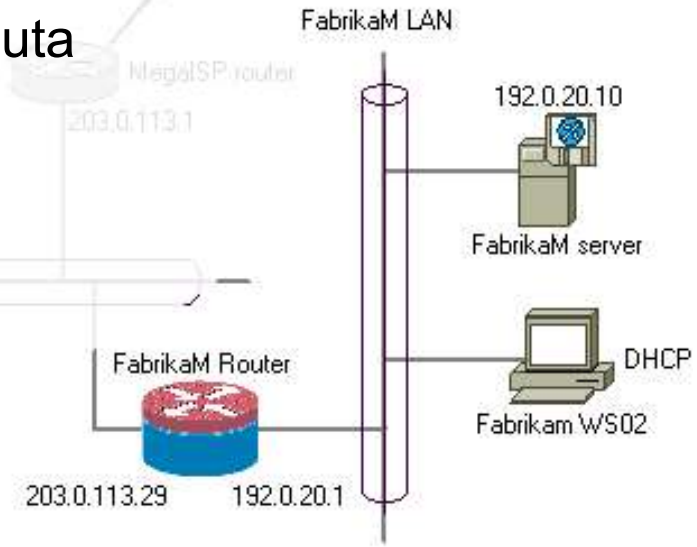
Mreža Contoso

- Centralna firma
- Simuliramo uobičajene mrežne servise koji se dele sa drugim klijentima:
  - www.contoso.com
  - ftp.contoso.com
  - mail.contoso.com



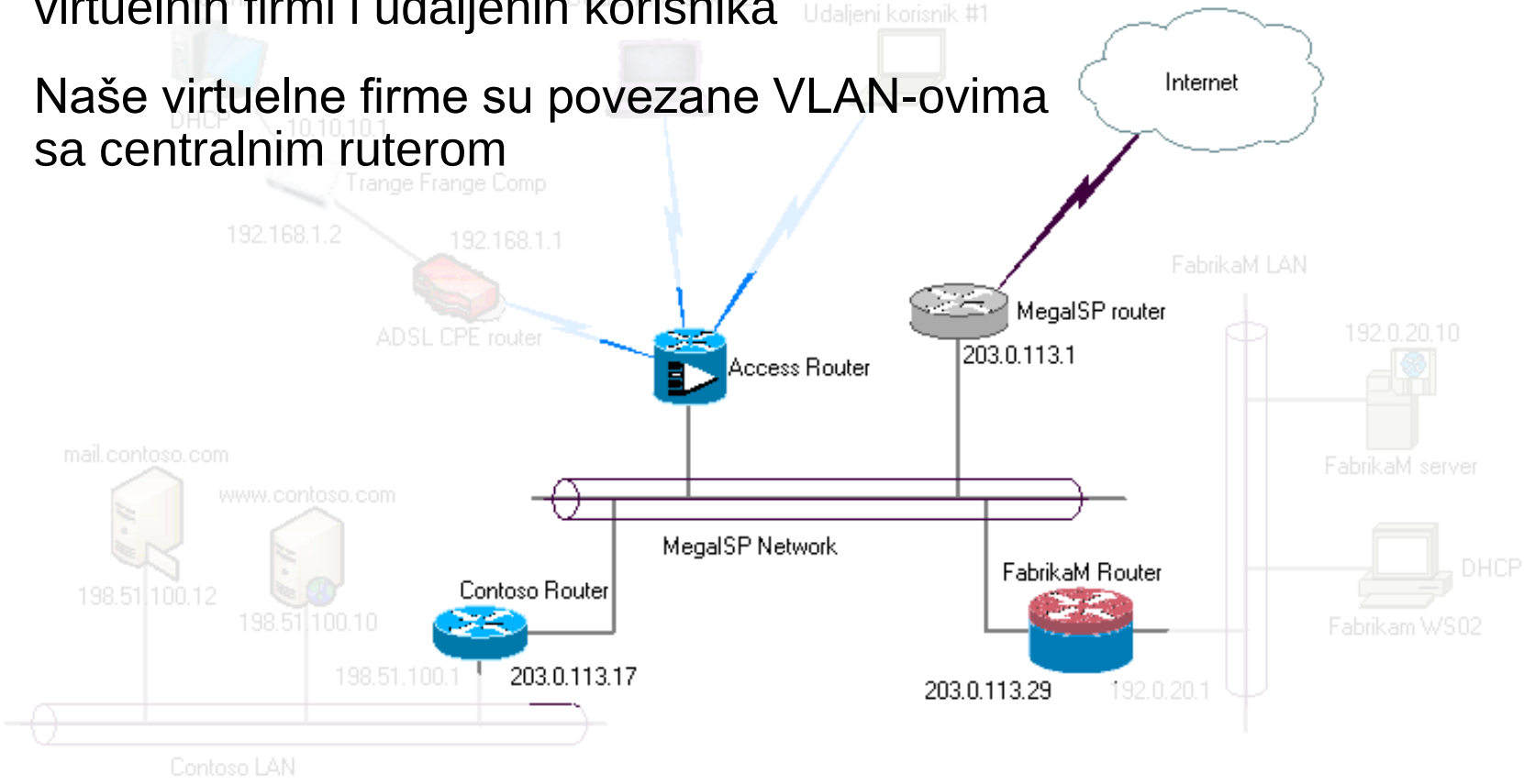
FabrikaM deo

- Partnerska firma ili udaljena lokacija
- Potrebno je da možemo da kontaktiramo centralnu lokaciju, čiji resursi nisu dostupni preko Interneta
- FabrikaM server je Mikrotik RouterOS virtuelna mašina, koja na svakih 10 minuta izvršava skript koji šalje e-pisma



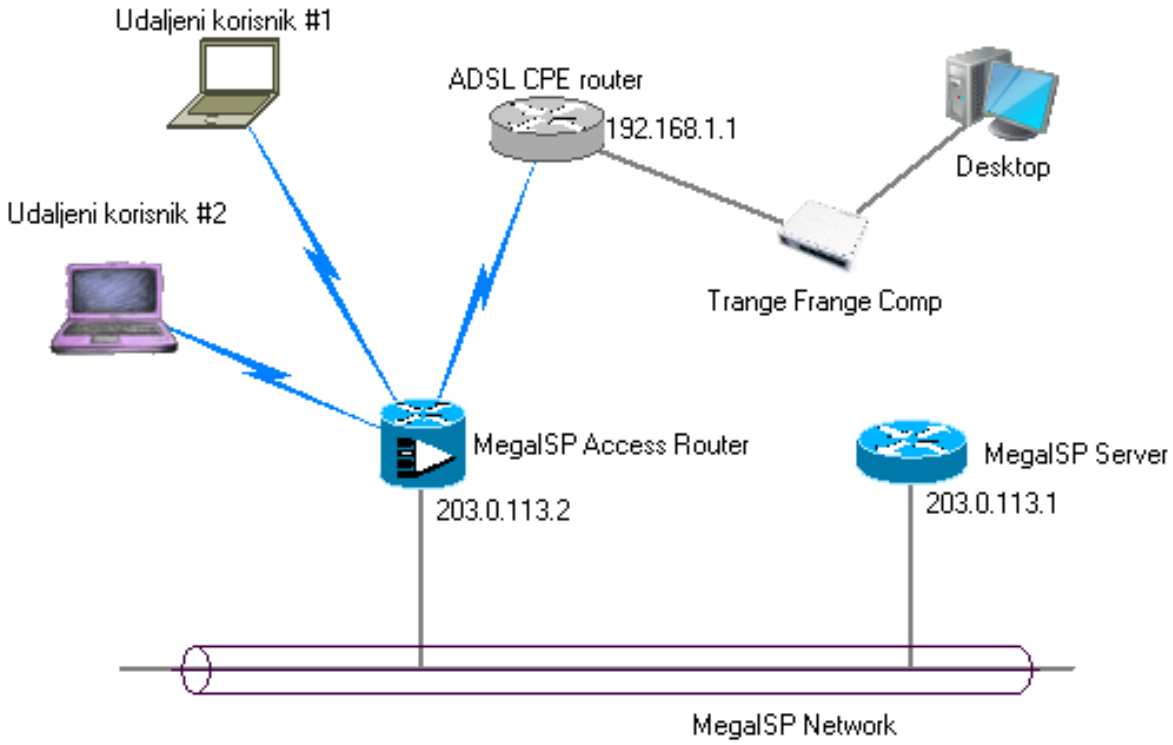
MegaISP dobavljač usluga

- Jednim virtuelnim dobavljačem usluga (ISP) smo simulirali sve Internet veze između naših virtuelnih firmi i udaljenih korisnika
- Naše virtuelne firme su povezane VLAN-ovima sa centralnim ruterom



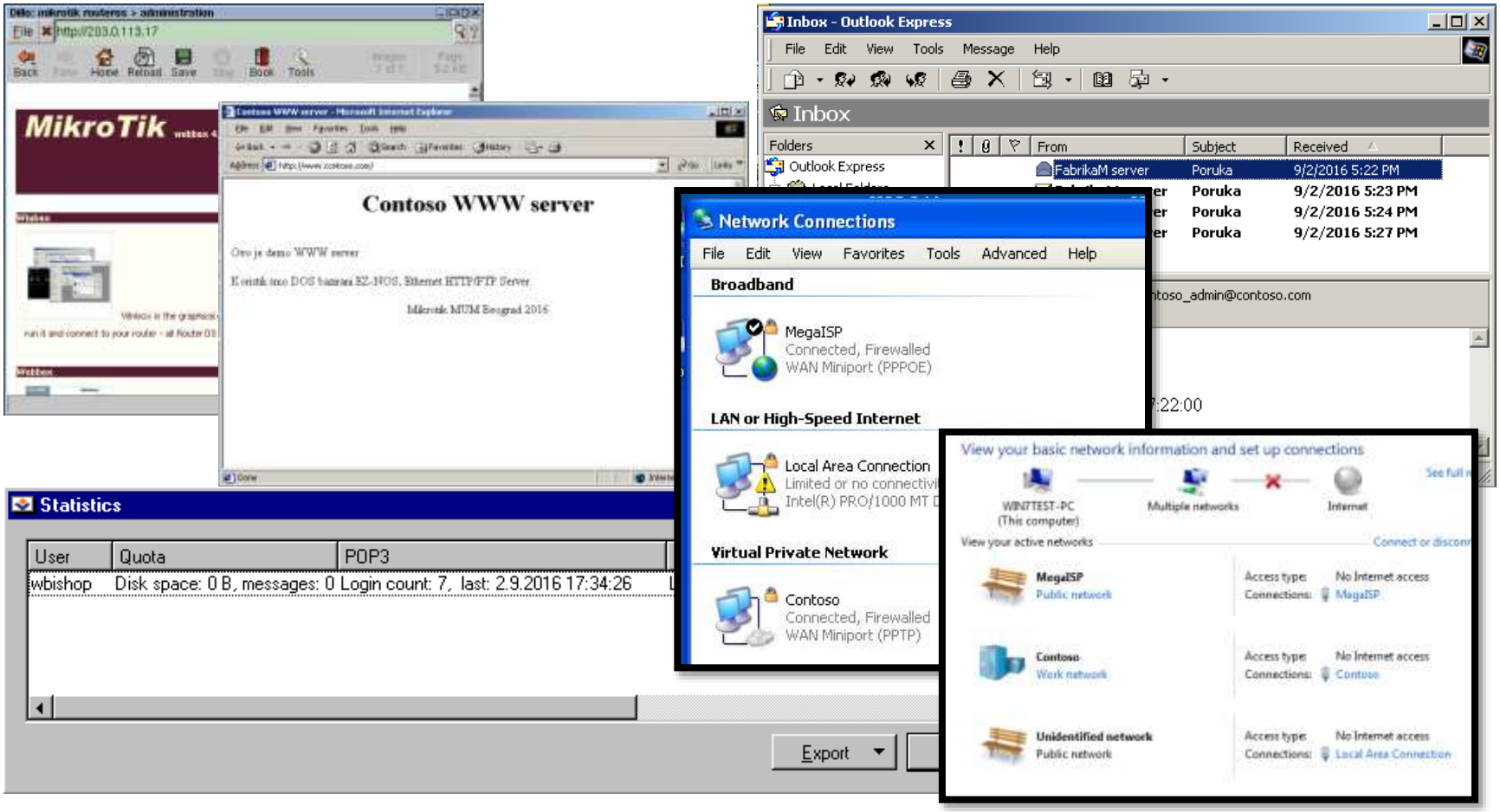
Udaljeni klijenti i „drumski ratnici“

- Simulirali smo kućne korisnike koji preko PPPoE (npr. ADSL povezivanje) se povezuju na operatera
- Dodali smo i jednu prosečnu firmu koja bi da “uštedi“ na troškovima Interneta i ima Mikrotik ruter iza ADSL rutera



Naša mreža bez IPSec-a i tunela

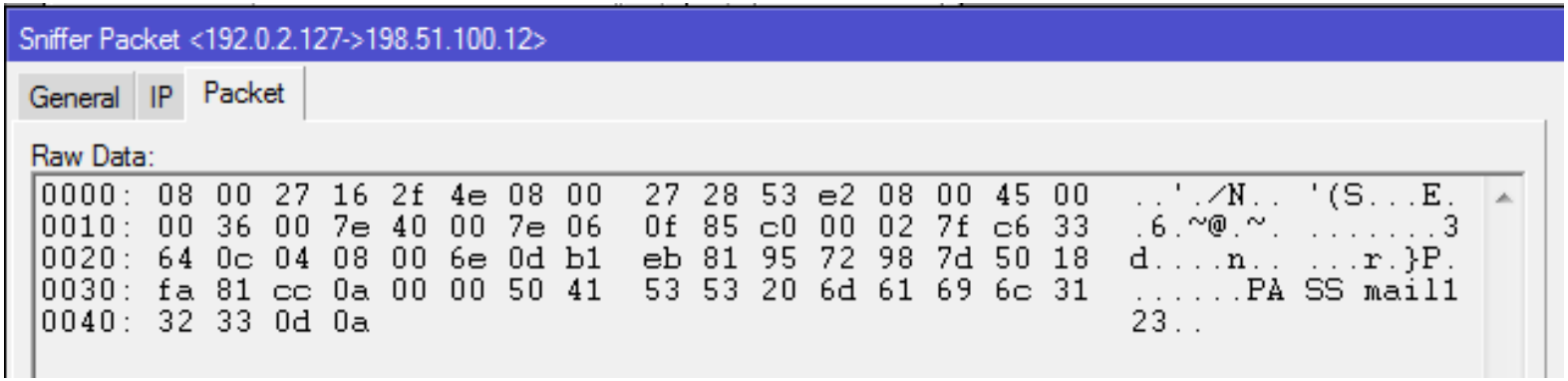
- Postavili smo celu laboratoriju bez ograničenja i testirali rad

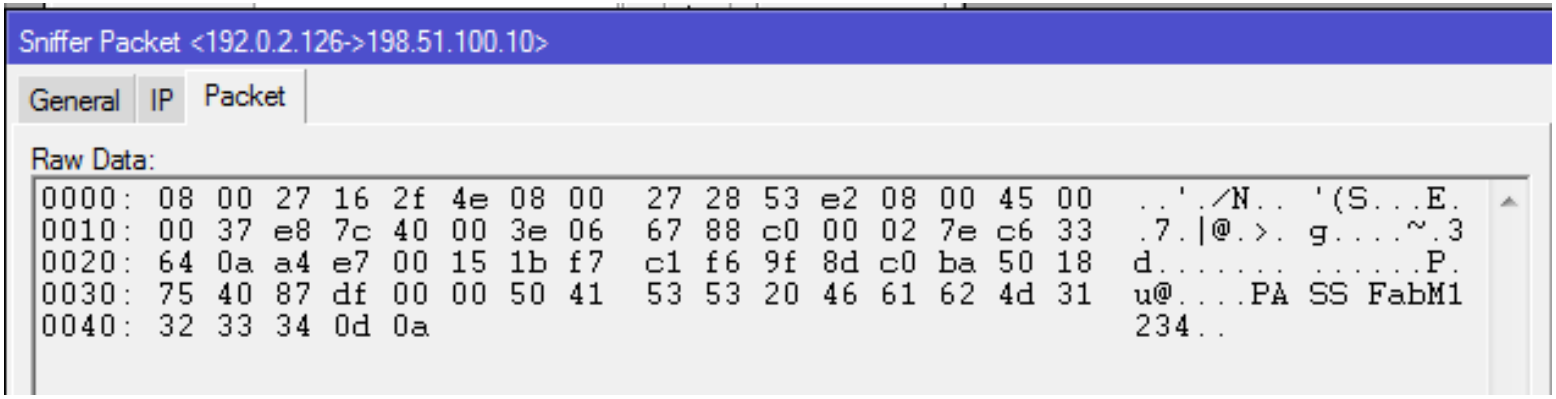


Site-to-site IPSec

Zašto nam treba zaštitni tunel?

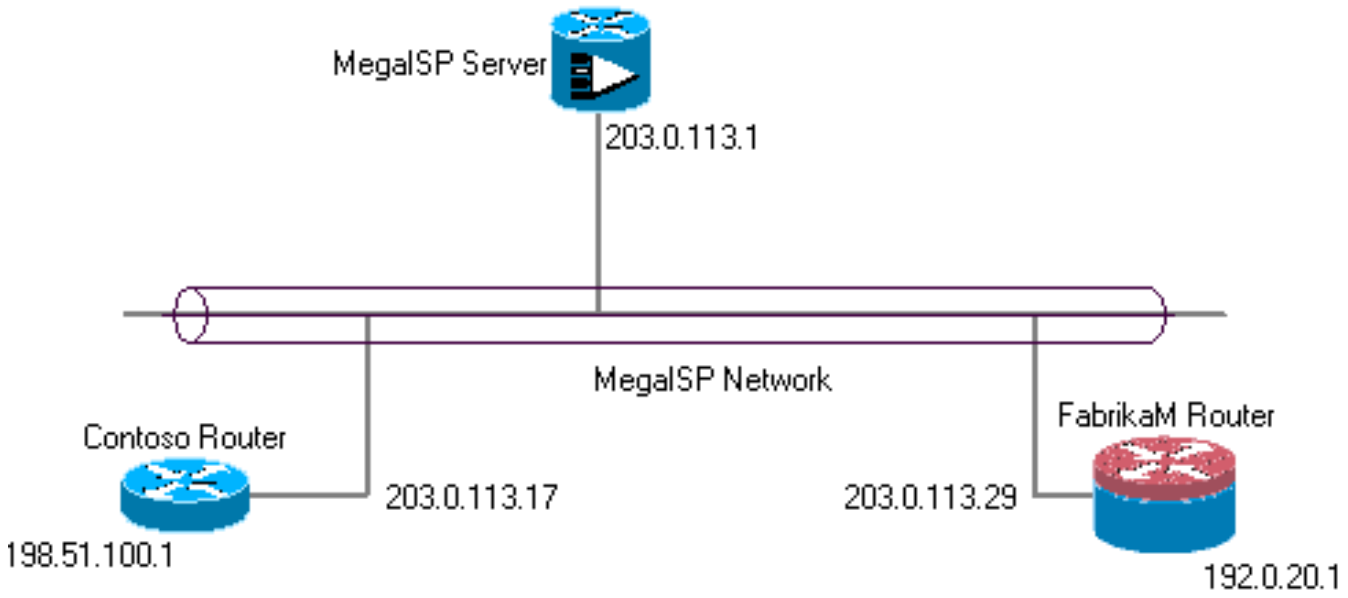
- Većina servisa nije predviđena za šifrovanje podataka
- Maliciozne osobe mogu da presretnu saobraćaj i dođu do podataka koji se razmenjuju





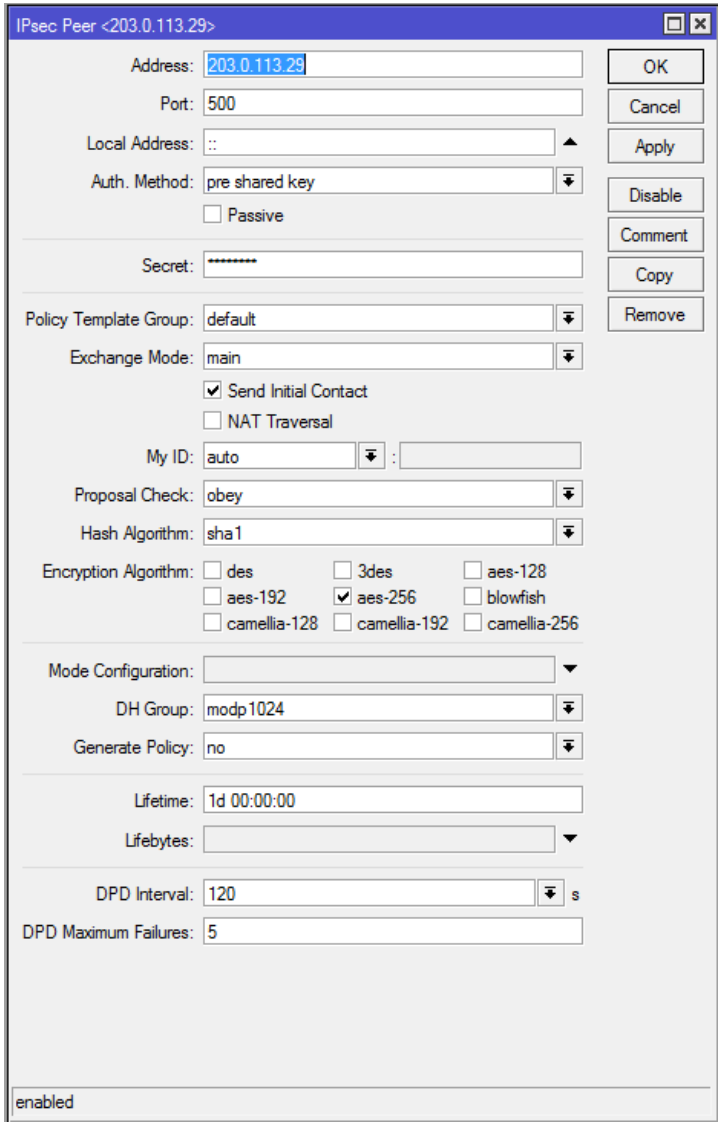
IKE phase I

- U ovoj fazi treba da definišemo parnjake (peers) koji će međusobno komunicirati
- Između ova dva uređaja će se uspostaviti saobraćaj i oni će formirati dinamički tunel



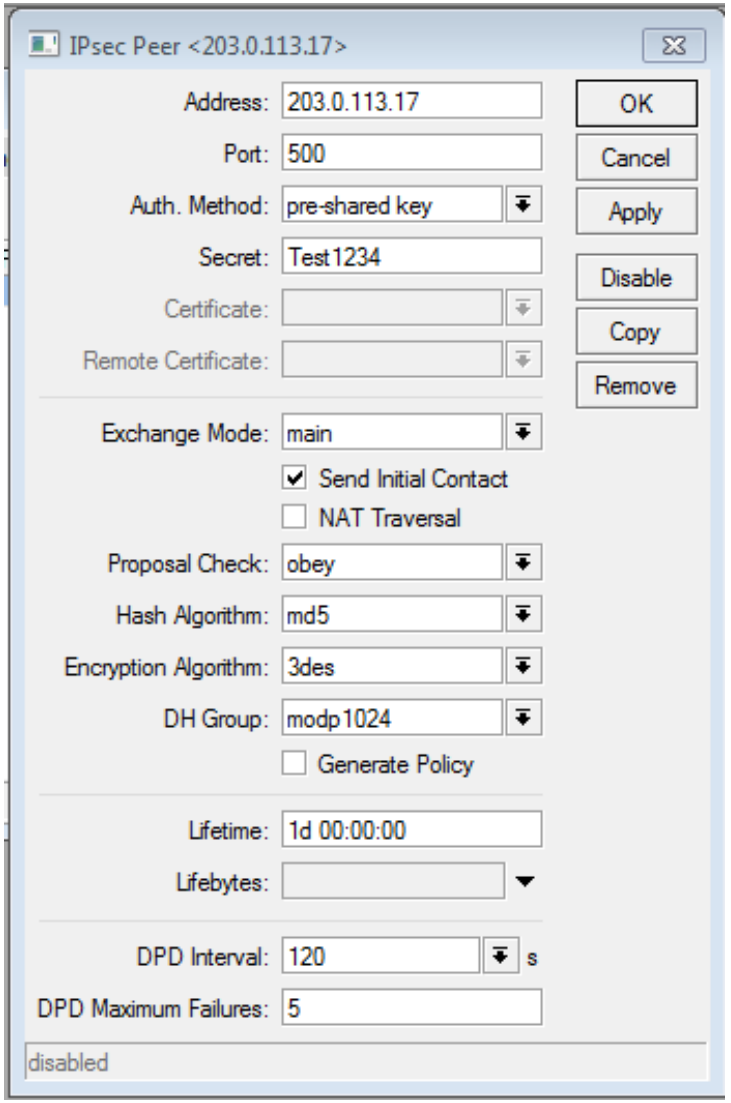
Contoso ruter

- Definišemo najpre parnjaka – FabrikaM ruter (203.0.113.29)
- Lozinka bi trebalo da bude rečenica (passphrase)
- Svi parametri koje ne unesemo će dobiti podrazumevanu vrednost
- Možemo zadati i našu lokalnu IP adresu, ukoliko imamo više javnih IP adresa



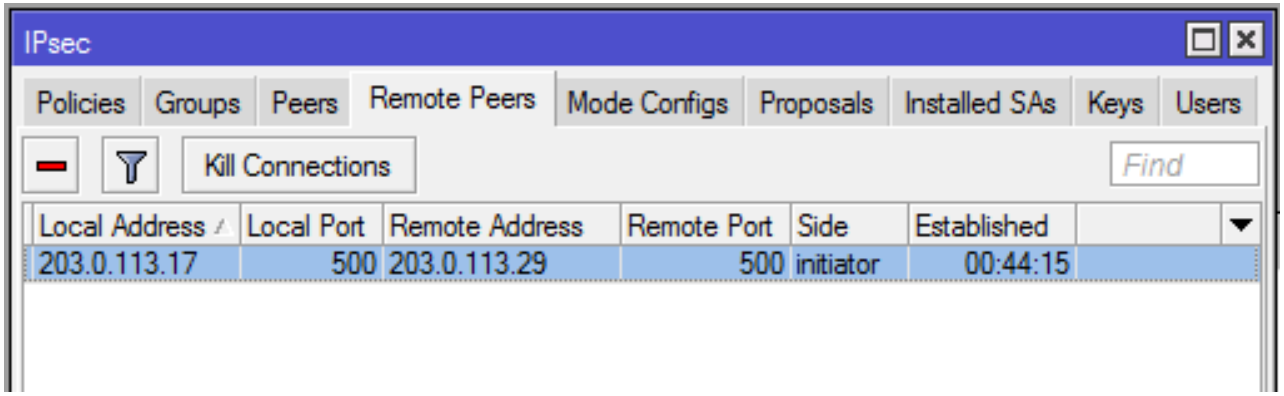
FabrikaM ruter

- Definišemo njegovog parnjaka – Contoso ruter (203.0.113.17)
- Ovde imamo stariju verziju RouterOS-a – v4.17
- Sintaksa je nešto drugačija, ali je osnova ista

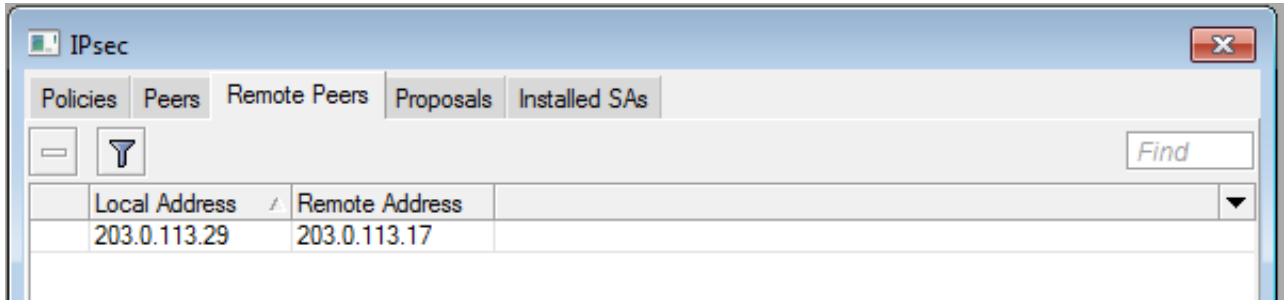


Proveravamo da li se tunel podigao

- Ukoliko smo dobro uneli parametre, tunel će se automatski podići
- Provera na strani Contoso rutera

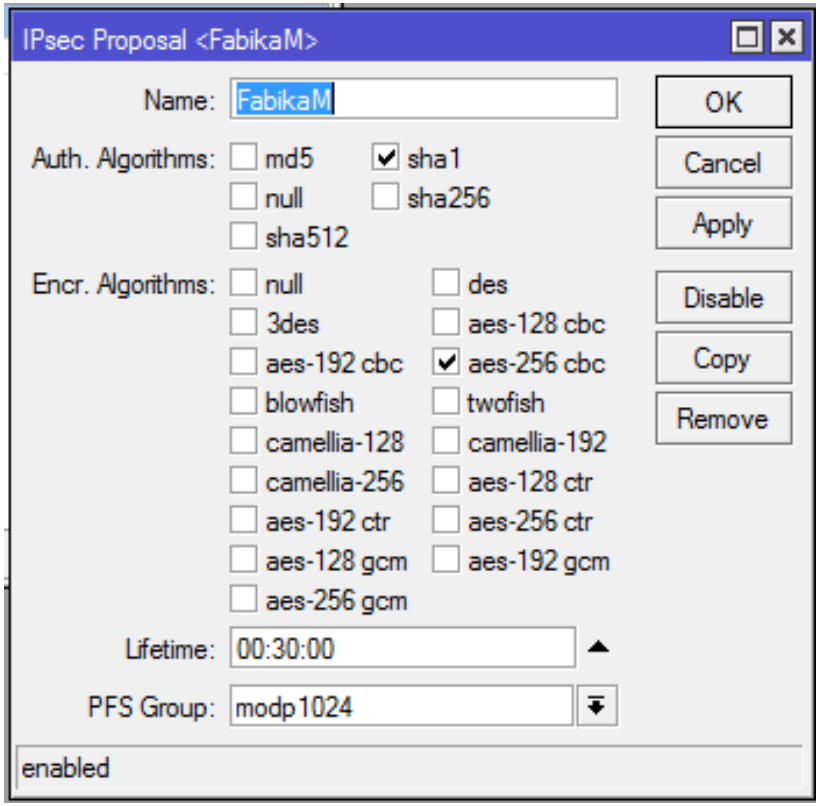


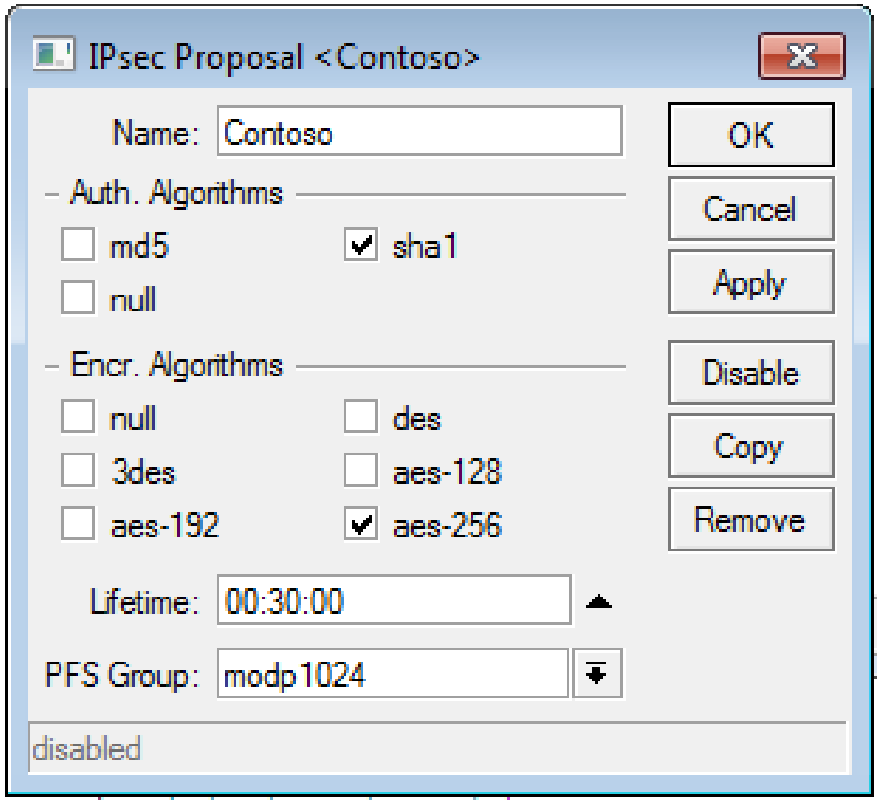
- Provera na strani FabrikaM rutera



Definisanje pravila šifrovanja saobraćaja

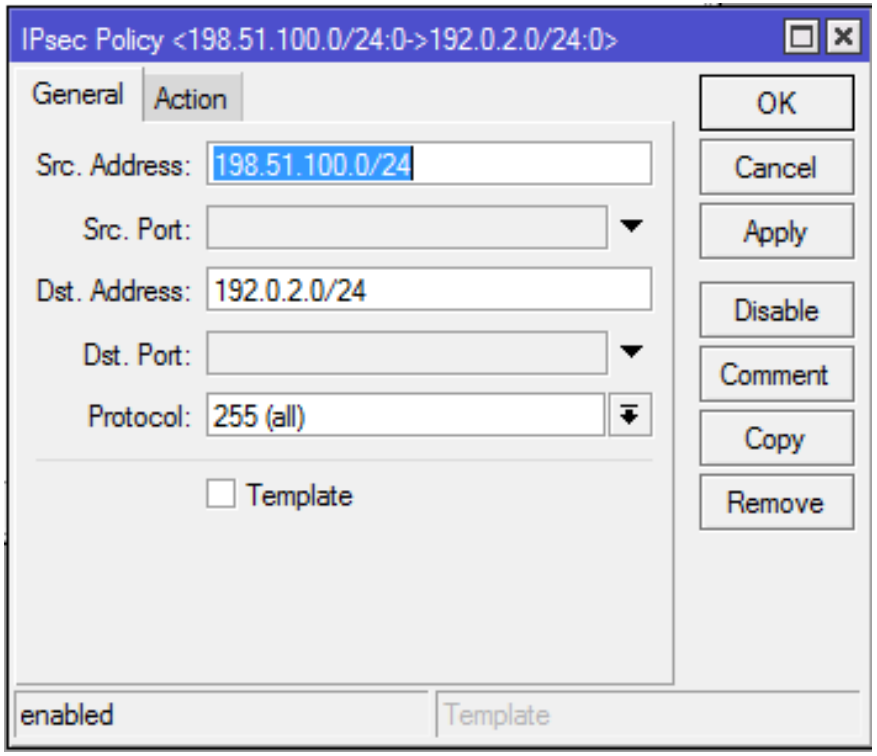
- Ovaj deo je identičan za obe strane
- Dodajemo novi skup pravila

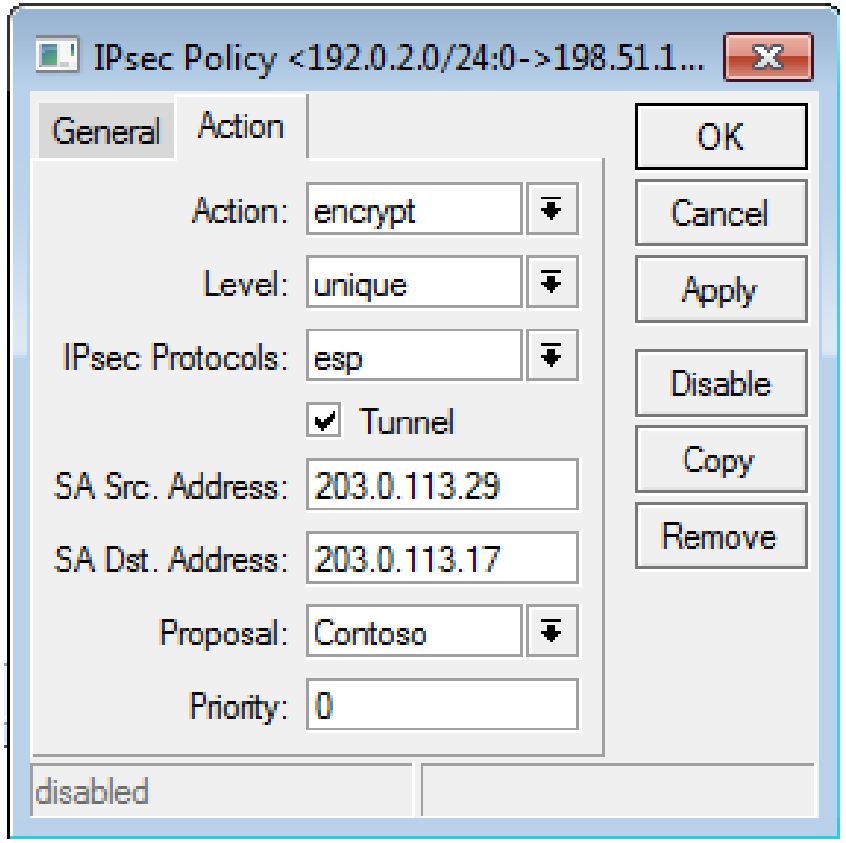




Interesantan saobraćaj za IPSec - policies

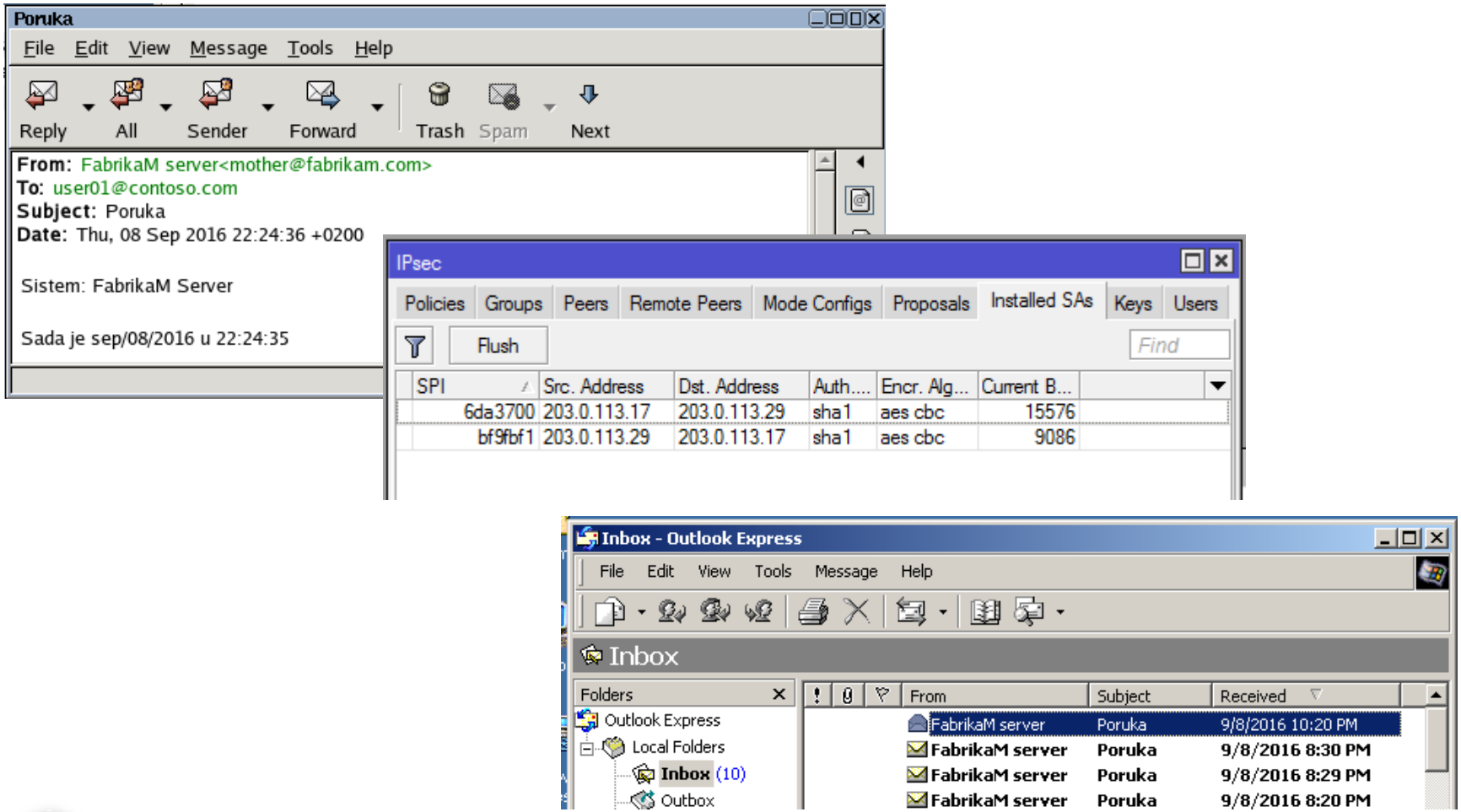
- Ovde treba da zadamo uslove koji će saobraćaj poslati u tunel
- Svaka polisa **mora** da bude identična na obe strane





Tunel je uspostavljen

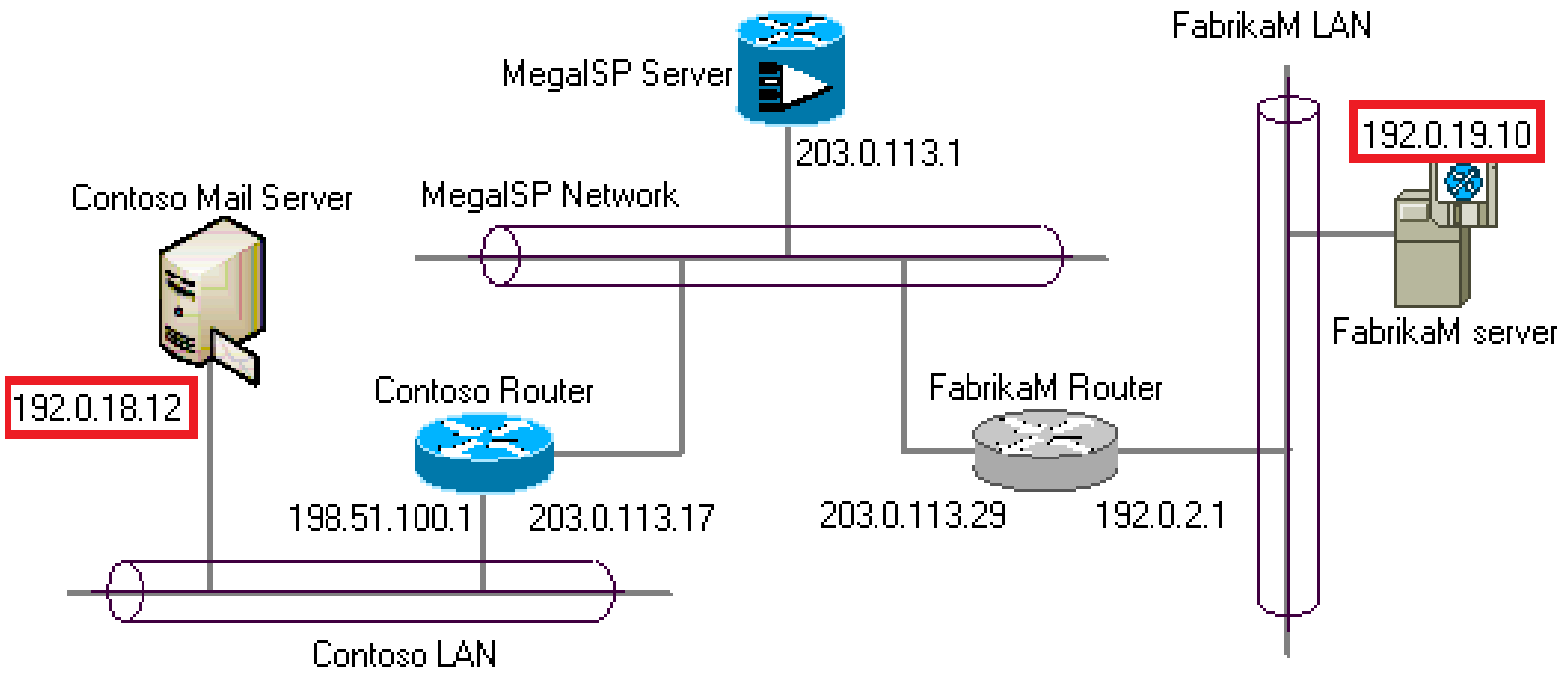
- Tunel će se podići čim krene saobraćaj



Site-to-site IPSec
sa NAT adresama servera

Promena originalnih IP adresa po zahtevu korisnika

- Imamo slučaj kada dve organizacije treba da komuniciraju, ali ne žele da koriste svoje interne adrese
- Moramo prvo da uradimo NAT, a zatim te adrese da pustimo u tunel



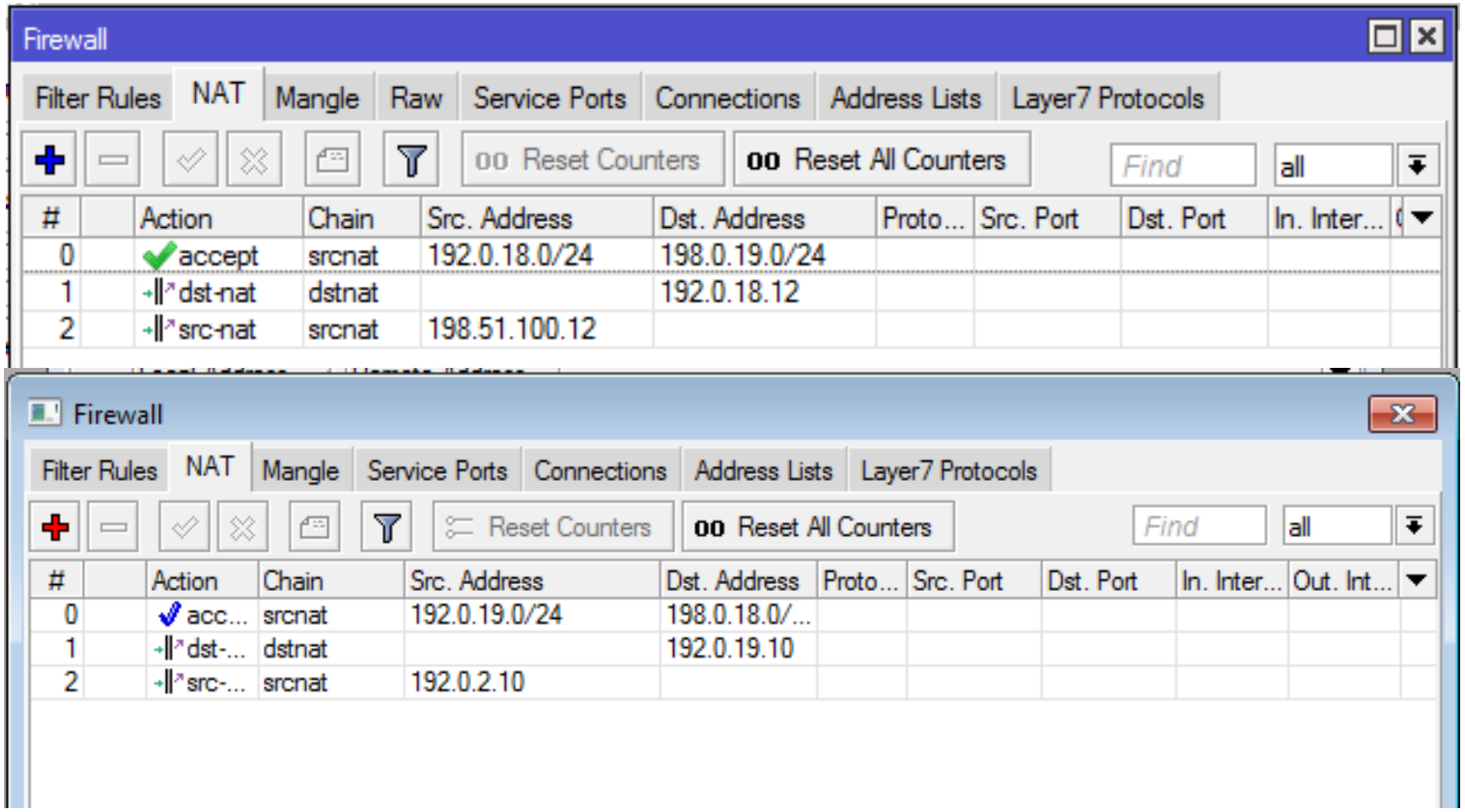
Plan za realizaciju zahteva

- Proces se zasniva na sledećem:

1. Napraviti DST-NAT pravilo za sve servere
2. Napraviti SRC-NAT pravilo za sve servere
3. Dodati IPSec Peer (IKE I) podešavanja
4. Dodati IPSec Proposal (IKE II) podešavanja
5. Dodati IPSec polise (interesantan saobraćaj)

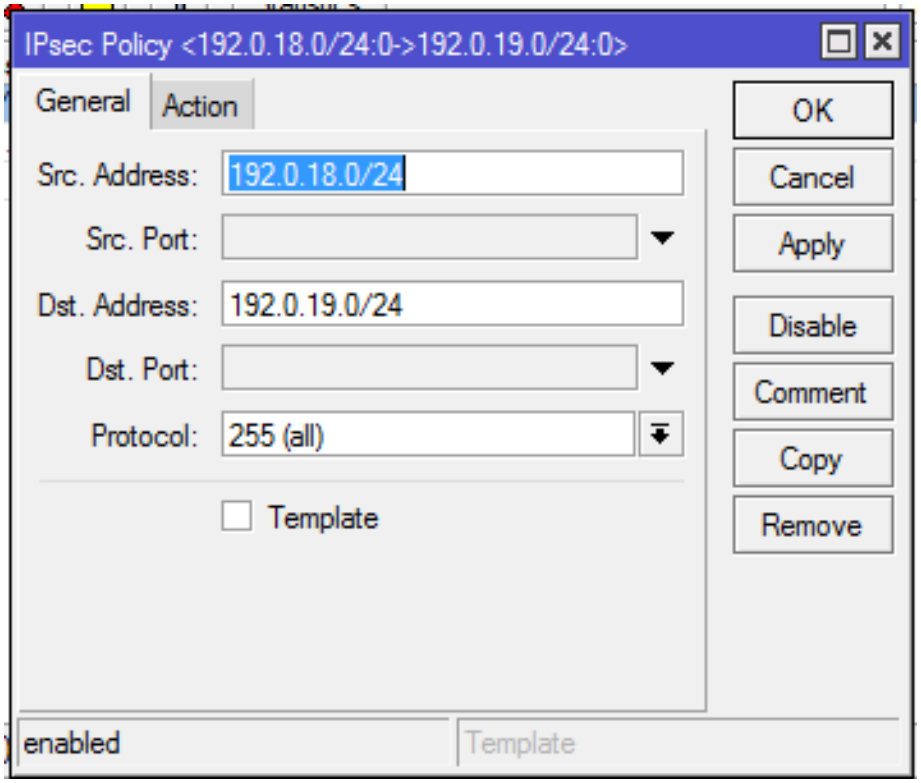
Definisanje NAT transformacije

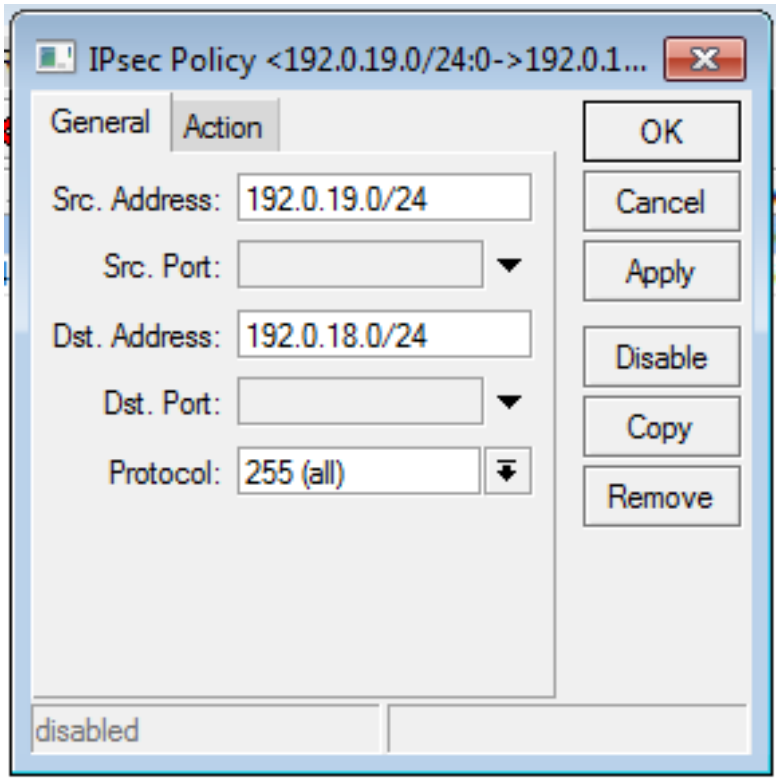
- U ovom slučaju imamo jedan korak više – NAT transformaciju
- NAT mora da se radi 1:1
- Ne zaboravite da propustite saobraćaj između NAT-ovanih mreža



Promena polisa za IPSec

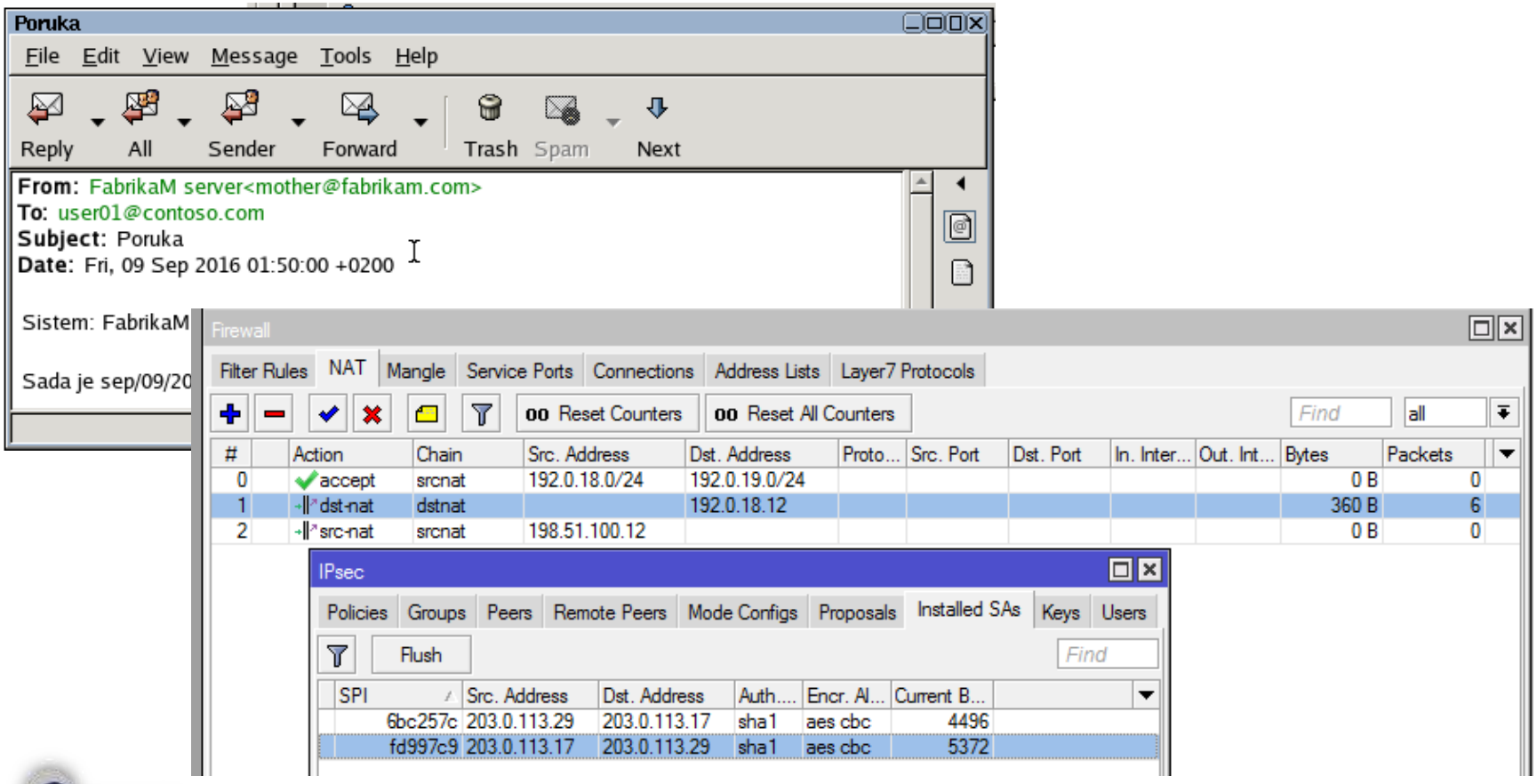
- Naša polisa će biti izmenjena u delu sa adresama koje iniciraju saobraćaj





Saobraćaj po novoj polisi

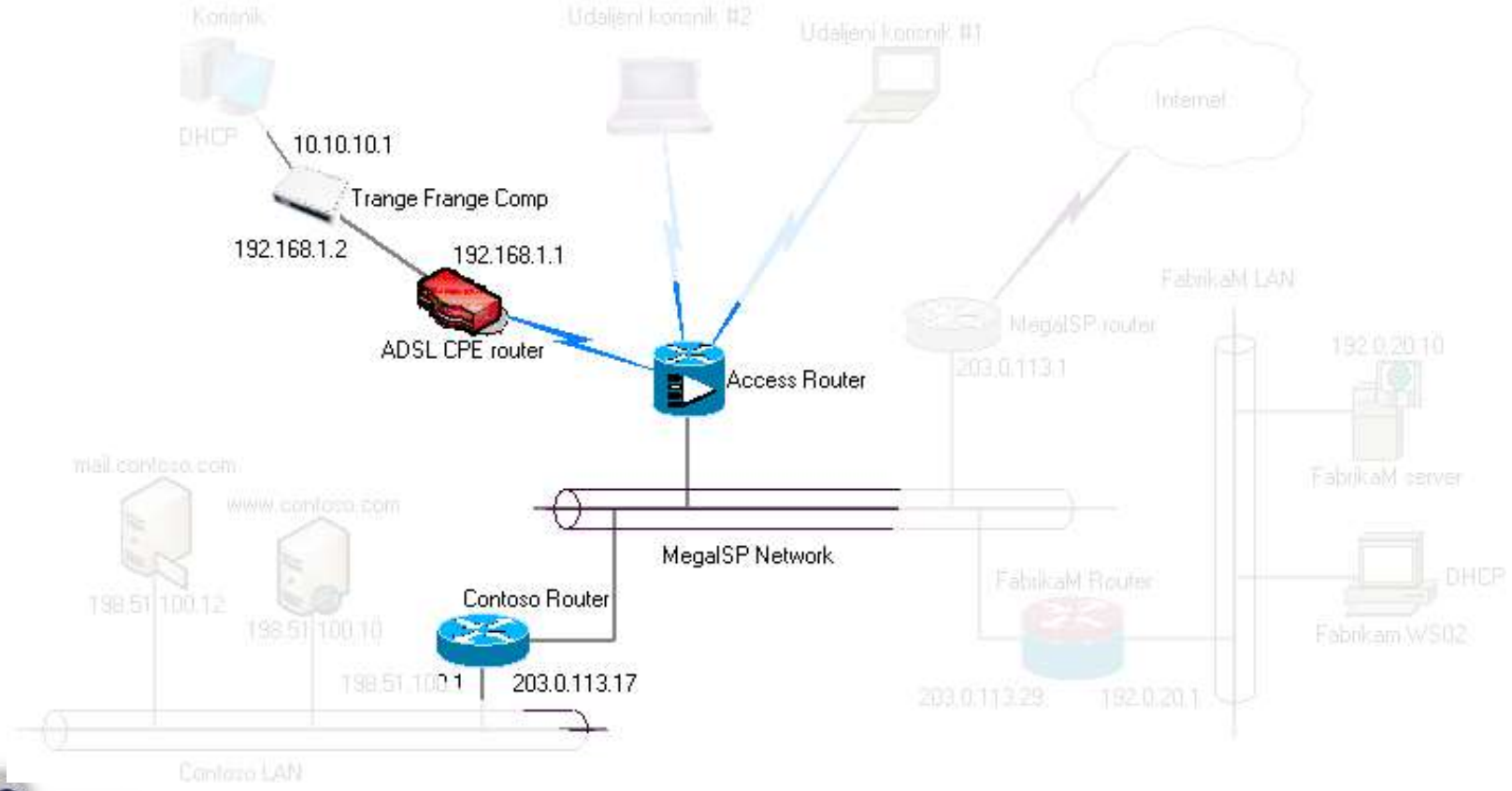
- Gasimo stare polise i puštamo nove
- Saobraćaj mora da ide opet kroz tunel



Site-to-Site IPSec
kada jedna strana ide kroz NAT

Jedna strana je iza NAT rutera

- Treba da se povežemo sa firmom koja ima IPSec ruter iza drugog rutera
- Udaljeni korisnik prolazi kroz NAT

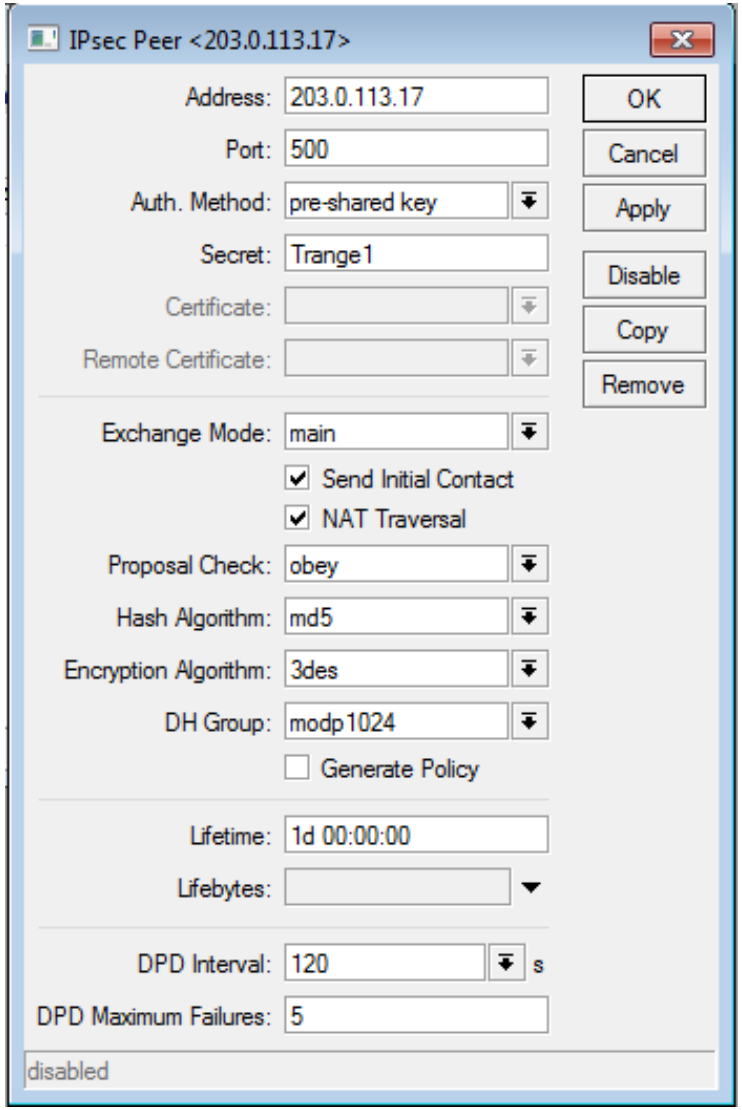


Problemi sa kojima se srećemo

- Dalja strana verovatno nema fiksnu IP adresu
- Javna adresa sa druge strane može da se promeni u bilo kom trenutku
- IPSec uređaj mora da prođe kroz NAT – menja se saobraćaj
- Kvalitet saobraćaja može da bude loš

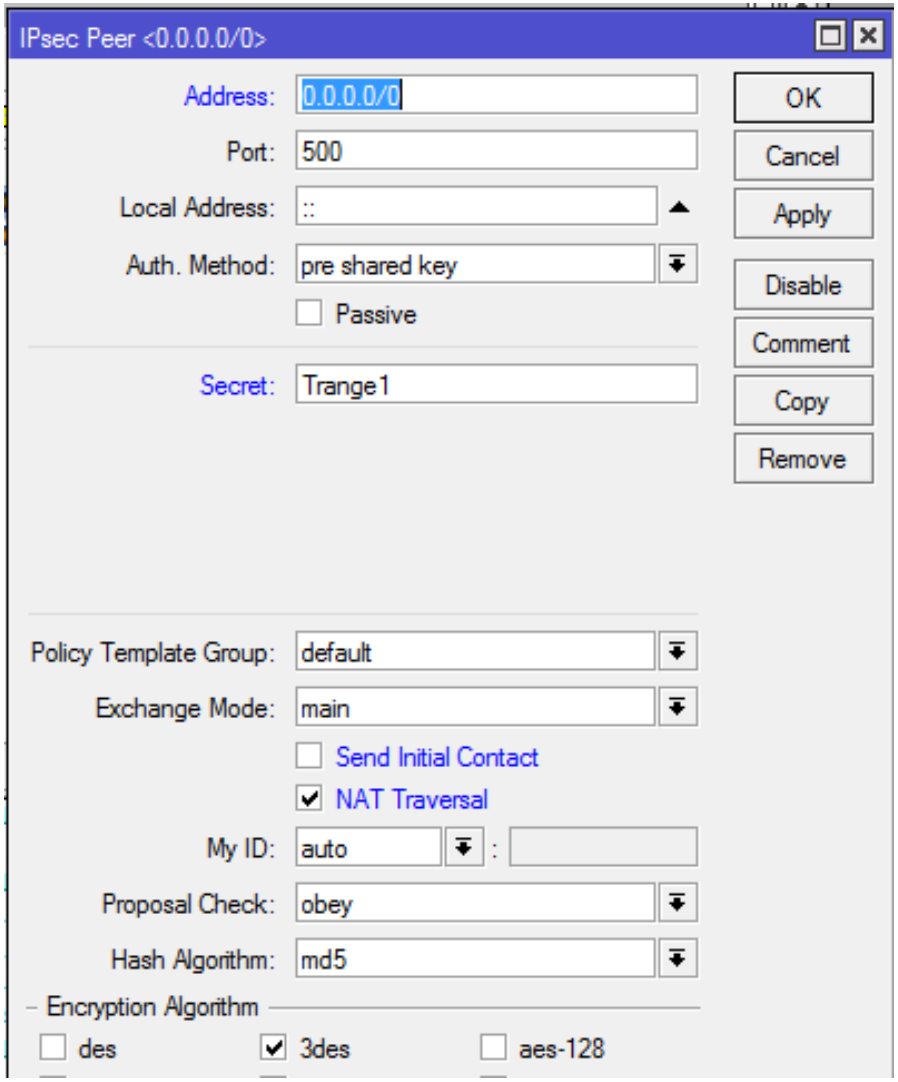
IKE faza I na strani iza NAT-a

- Na udaljenoj strani se sve pravi po istoj proceduri, pošto mi imamo javnu IP adresu
- Moramo da uključimo opciju **NAT traversal**
- Sve ostale parametre zadajemo da budu identični na obe strane



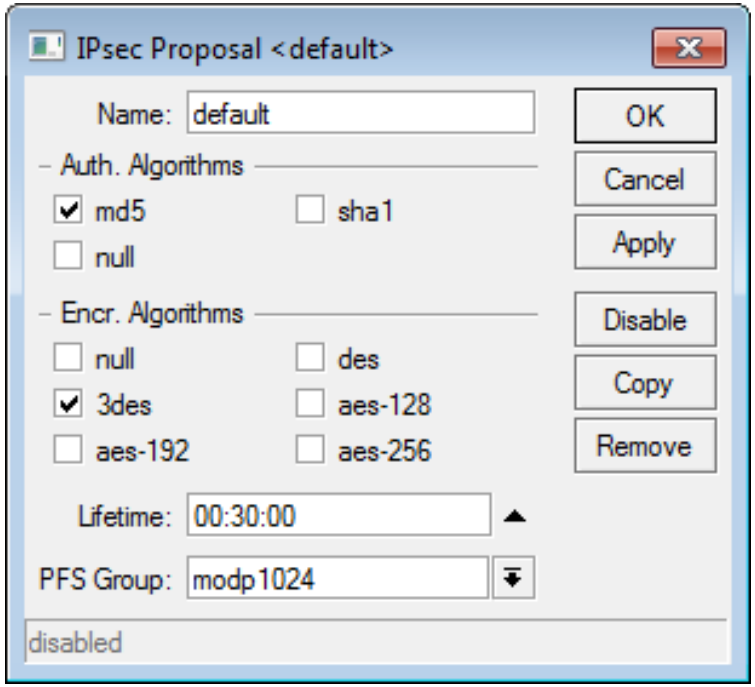
IKE faza I na našoj strani

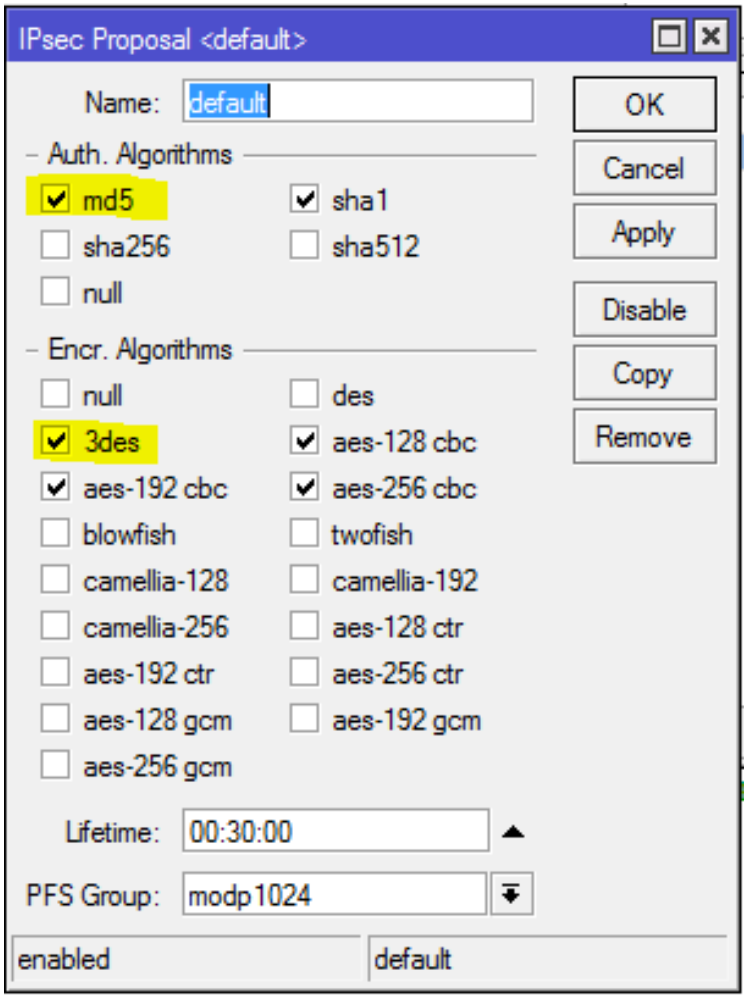
- Na našoj strani moramo da napravimo pravilo koje dozvoljava bilo koju adresu
- Moramo da uključimo opciju **NAT traversal**
- Sa naše strane moramo da uključimo opciju **Generate policy**
- Isključujemo opciju **Send Initial Contact**



IKE II parametri

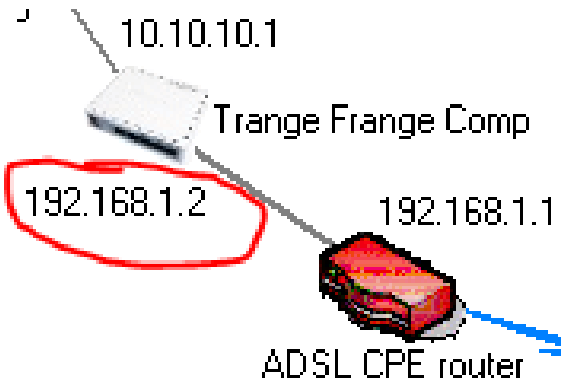
- Ove parametre pravimo na isti način kao i kod običnog IPSec saobraćaja
- Naša *default* polisa mora da pokrije sve parametre udaljenog uređaja

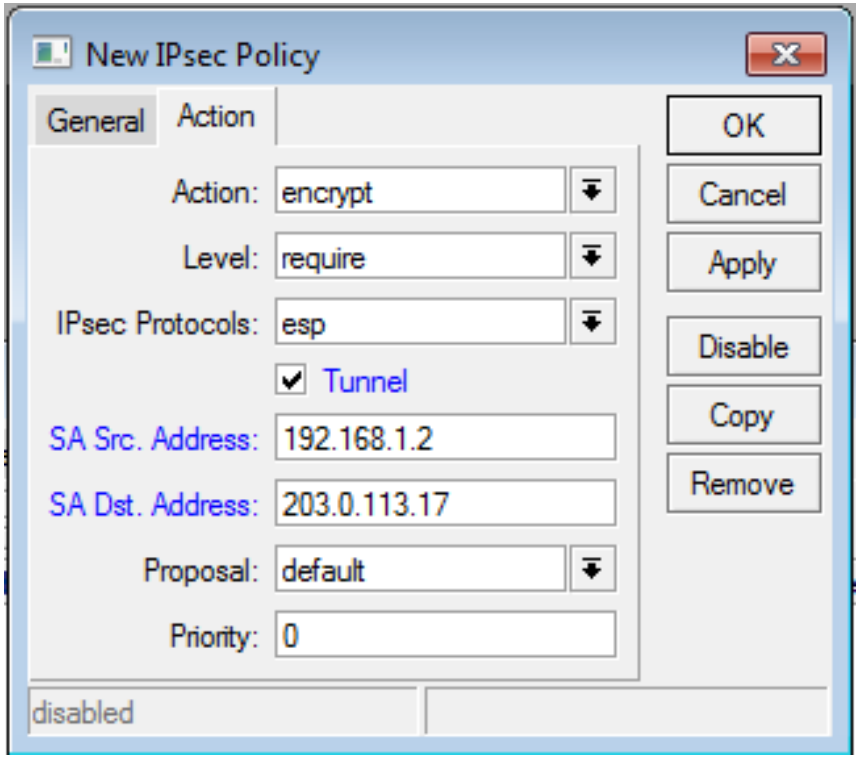




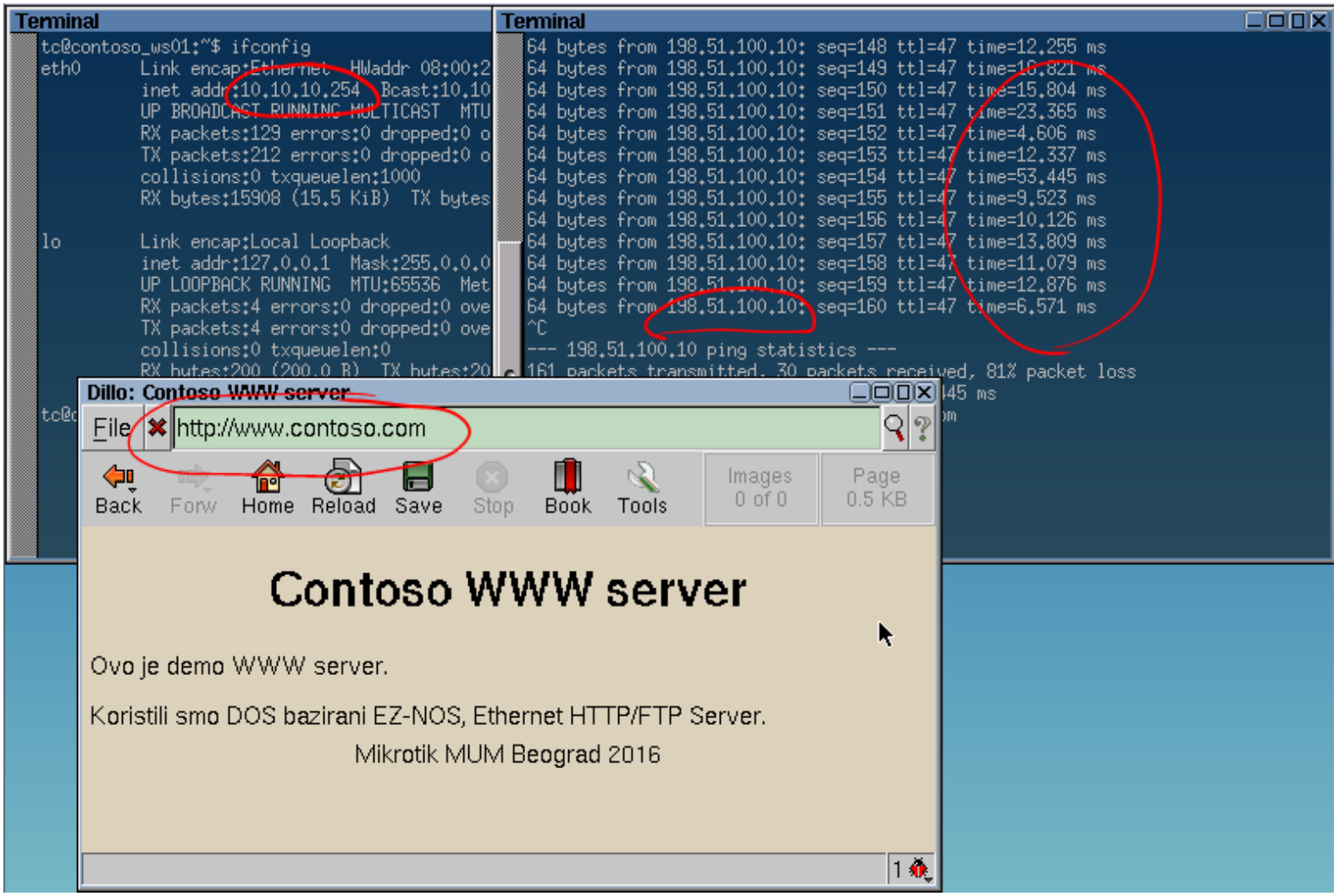
Polise za interesantan saobraćaj

- Polisa sa naše strane se ne pravi, već će je uređaj sam napraviti prilikom povezivanja
- Dodajemo zaobilaženje NAT-a za udaljeni opseg u `ip firewall nat` sekciji
- Početna adresa na udaljenoj strani je **privatna IP adresa izlaznog interfejsa**





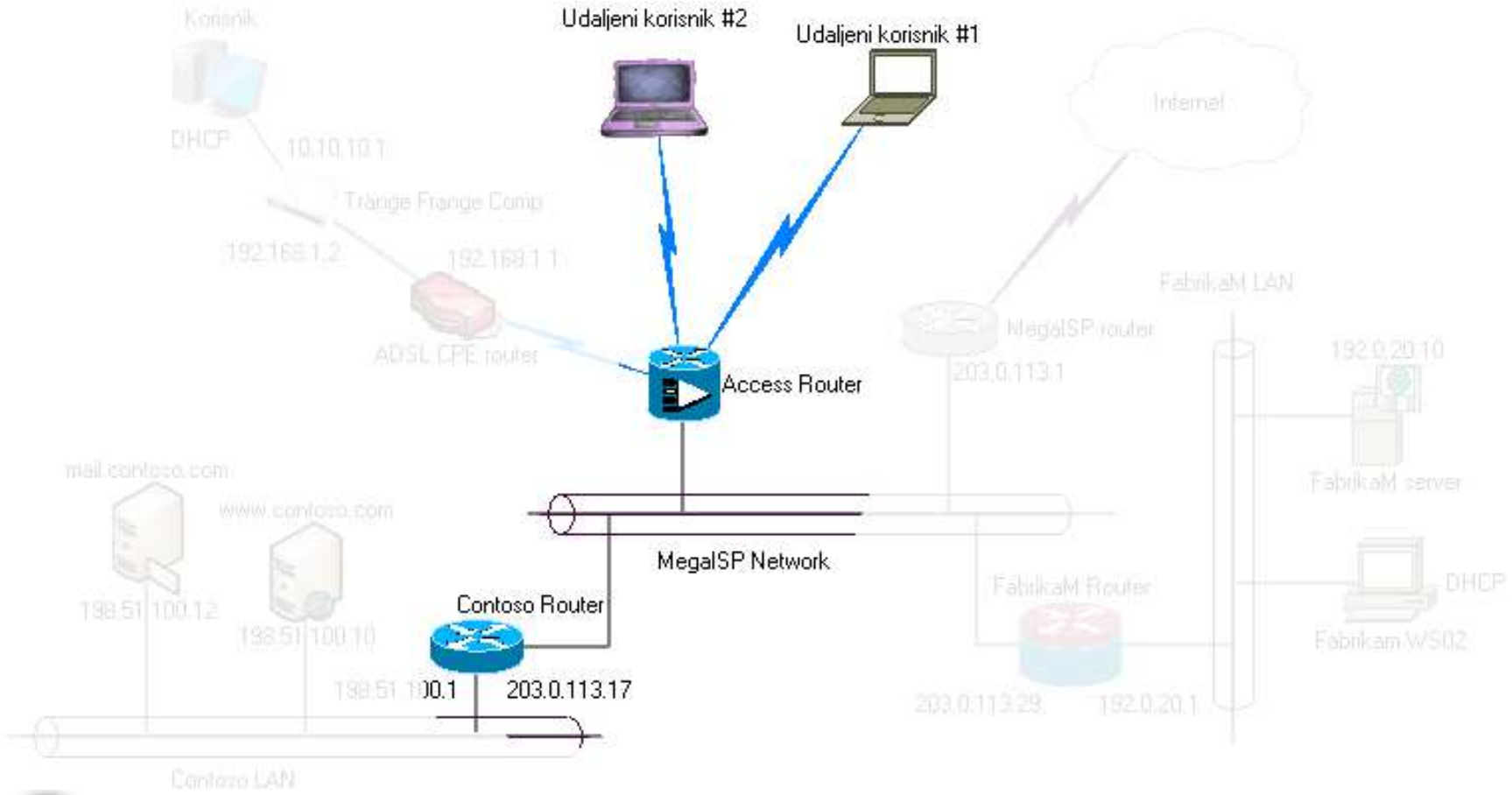
Tunel se podigao



L2TP/IPSec za „drumske ratnike“

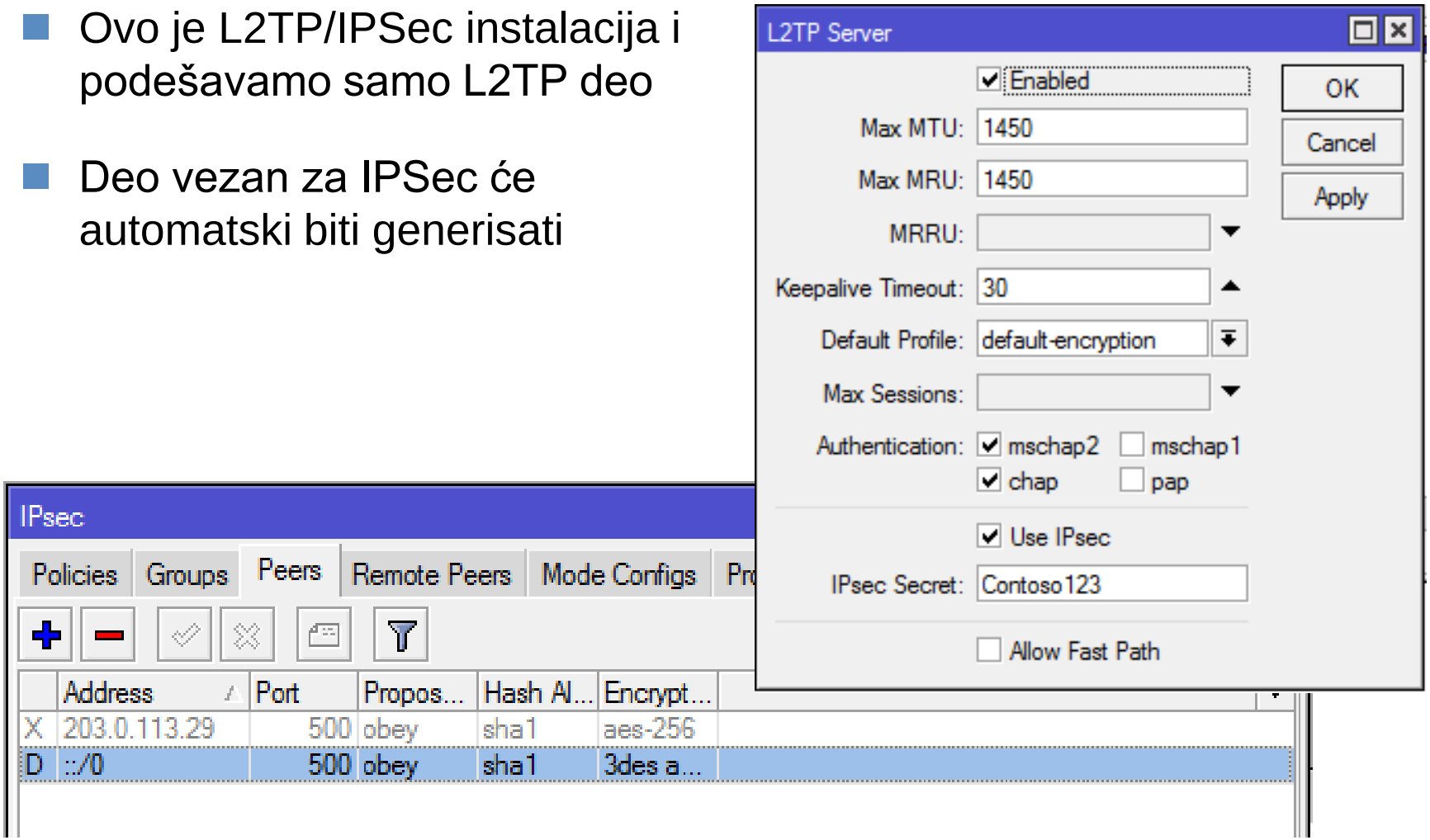
Povezujemo udaljene korisnike

- Korisnik je kod kuće, na putu, u gradu…
- Želimo zaštićenu vezu



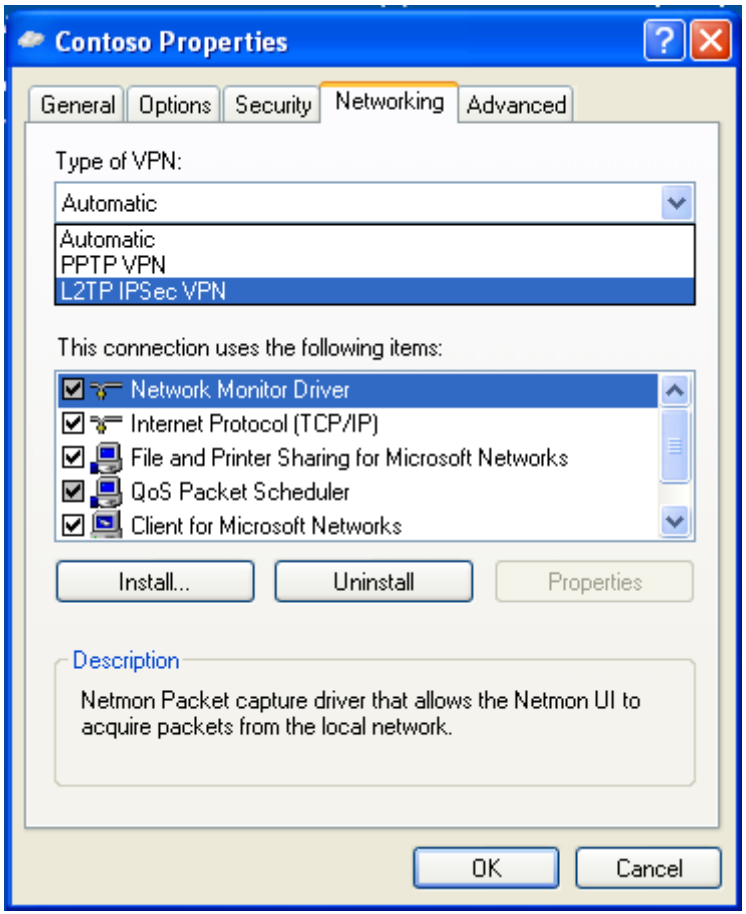
Pripremamo naš ruter

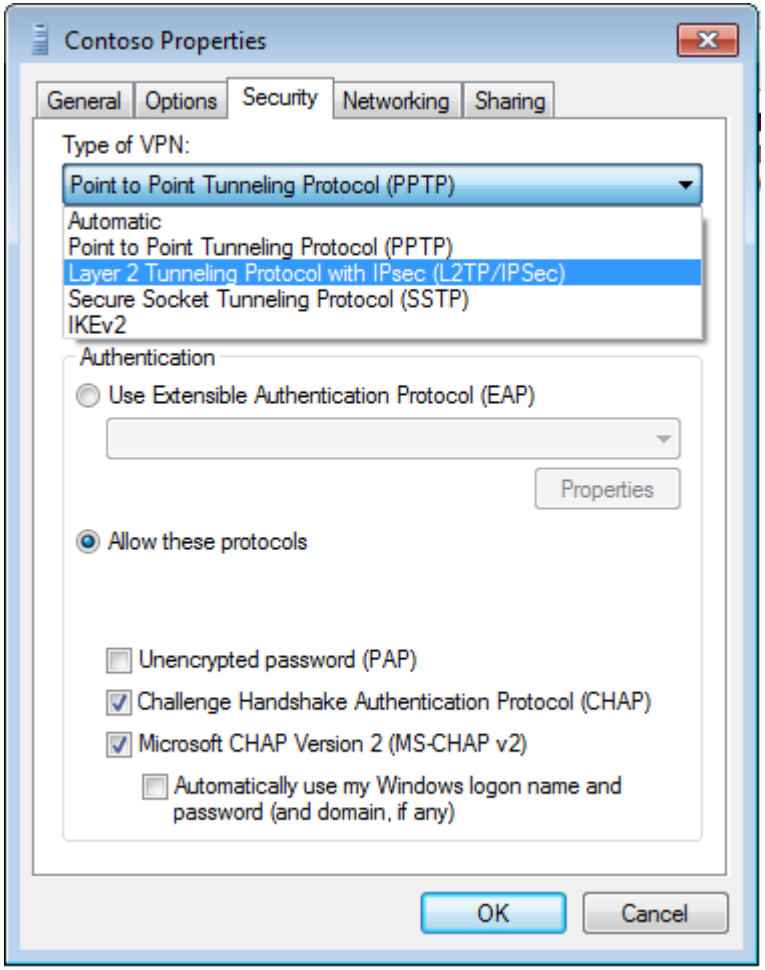
- Ovo je L2TP/IPSec instalacija i podešavamo samo L2TP deo
- Deo vezan za IPSec će automatski biti generisati



Podešavamo klijente

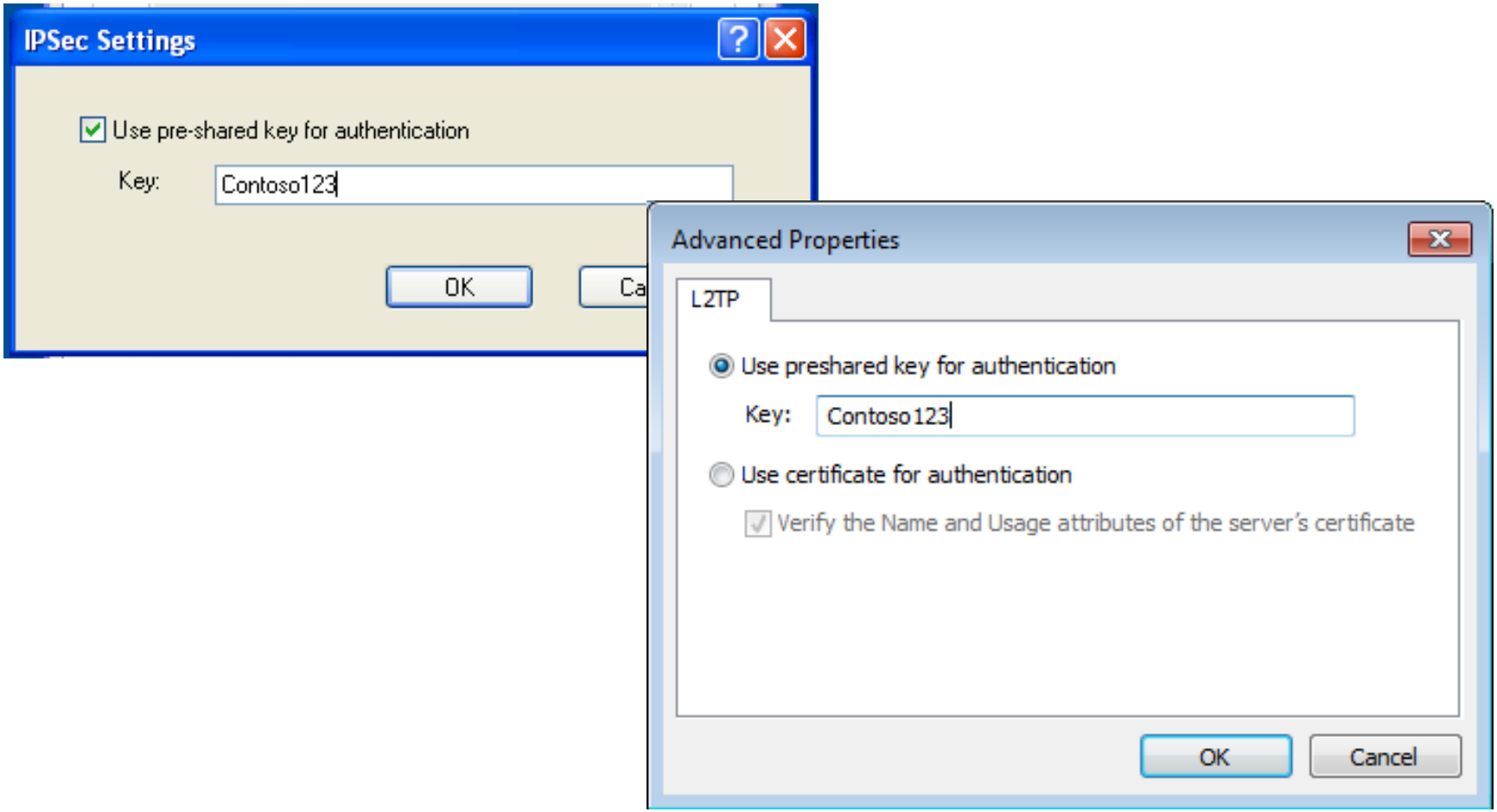
- Windows XP i noviji podržavaju L2TP/IPSec tunel





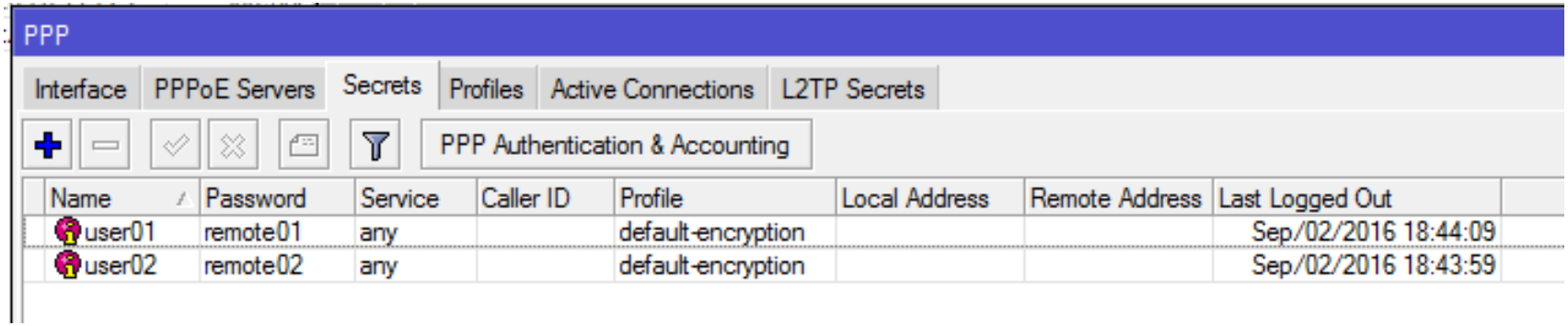
Podešavamo IPSec deljeni ključ

- Za IPSec fazu nam treba deljeni ključ



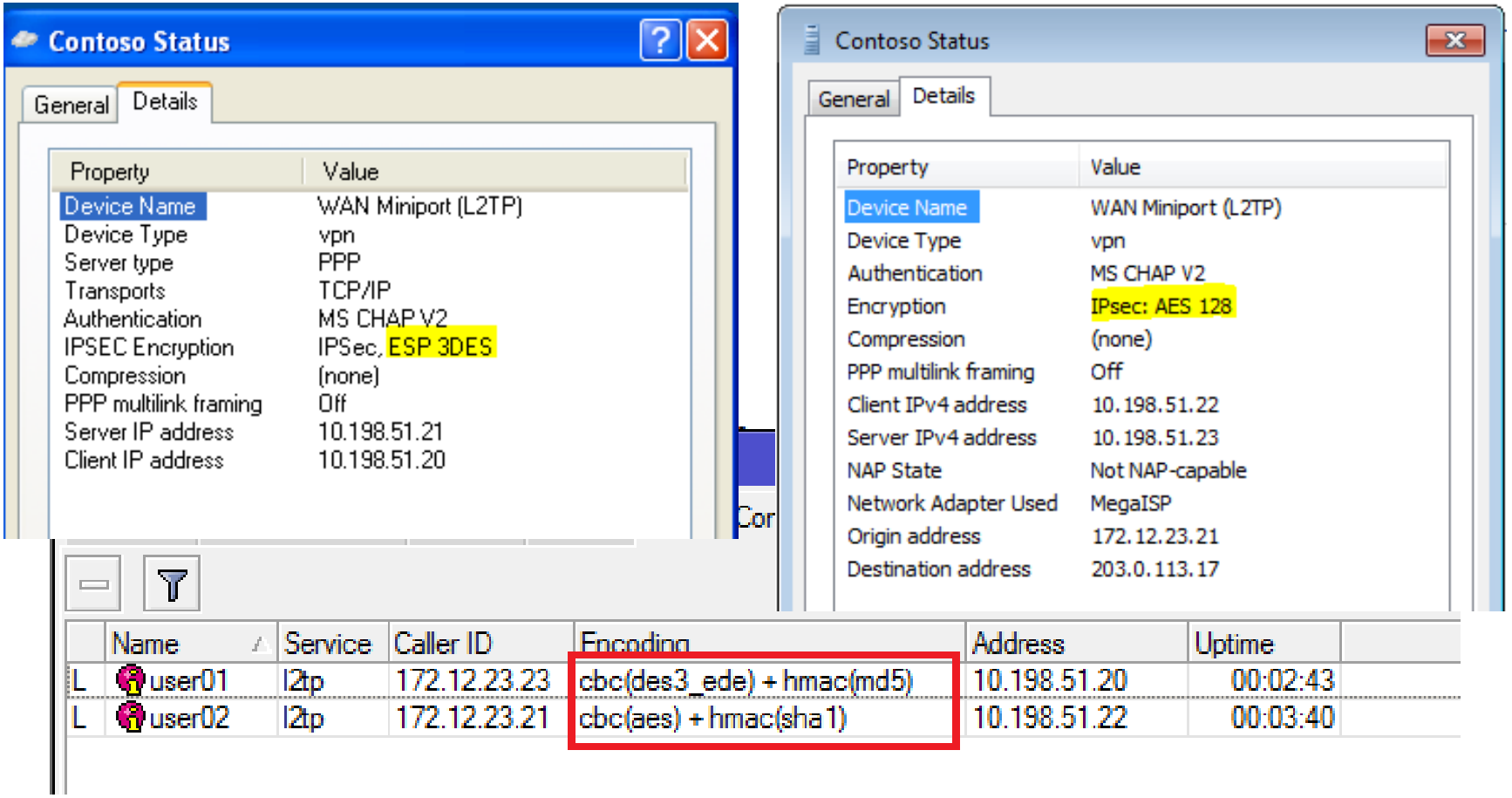
Nalozi za L2TP tunel

- L2TP VPN je deo PPP servisa
- PPP servisi imaju svoju bazu korisničkih naloga ili koriste RADIUS
- Ovi nalozi nisu povezani sa IPSec ključem



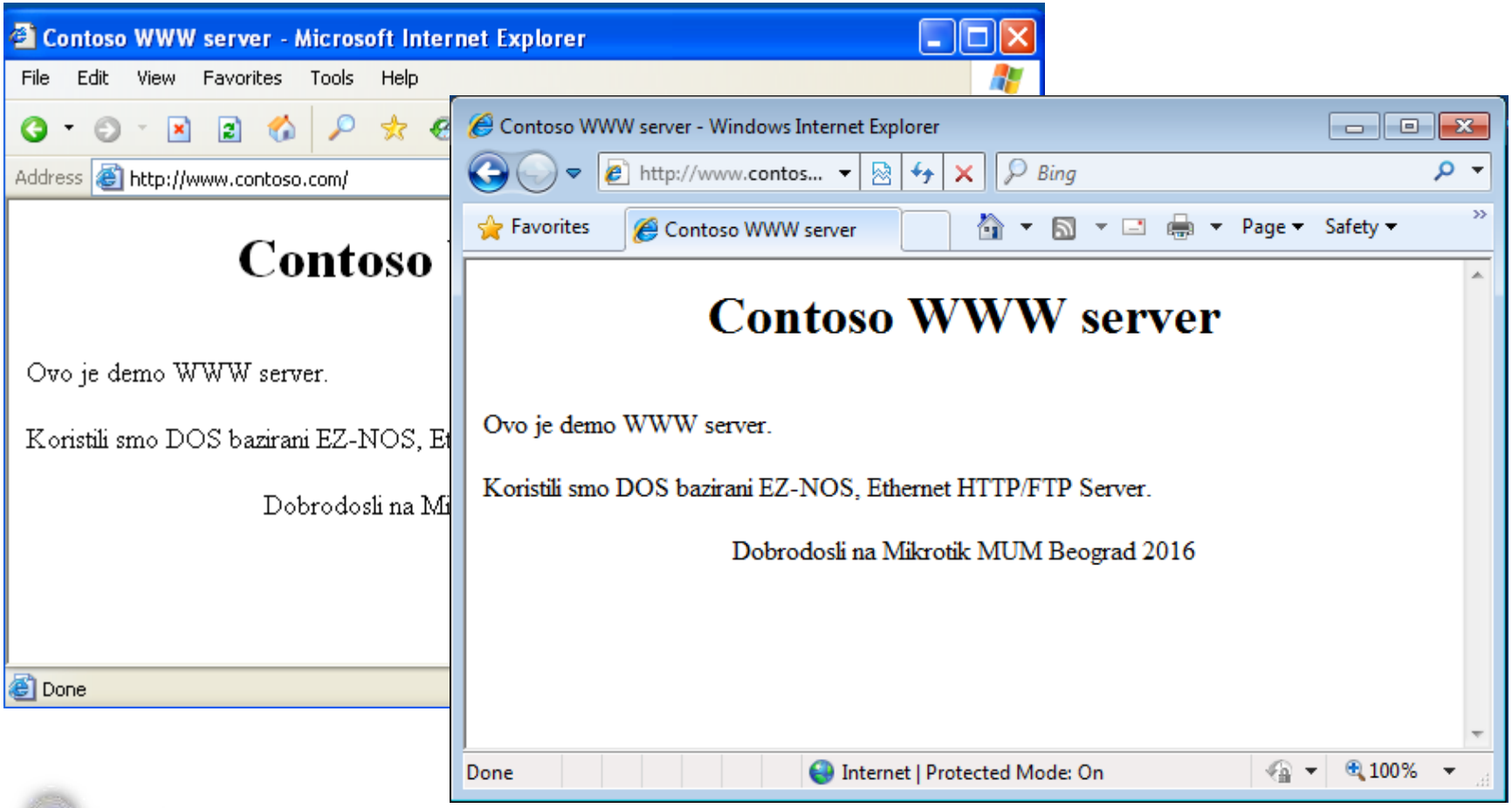
Povezujemo klijente

- Iniciraćemo VPN konekciju sa klijenata



Testiramo klijente

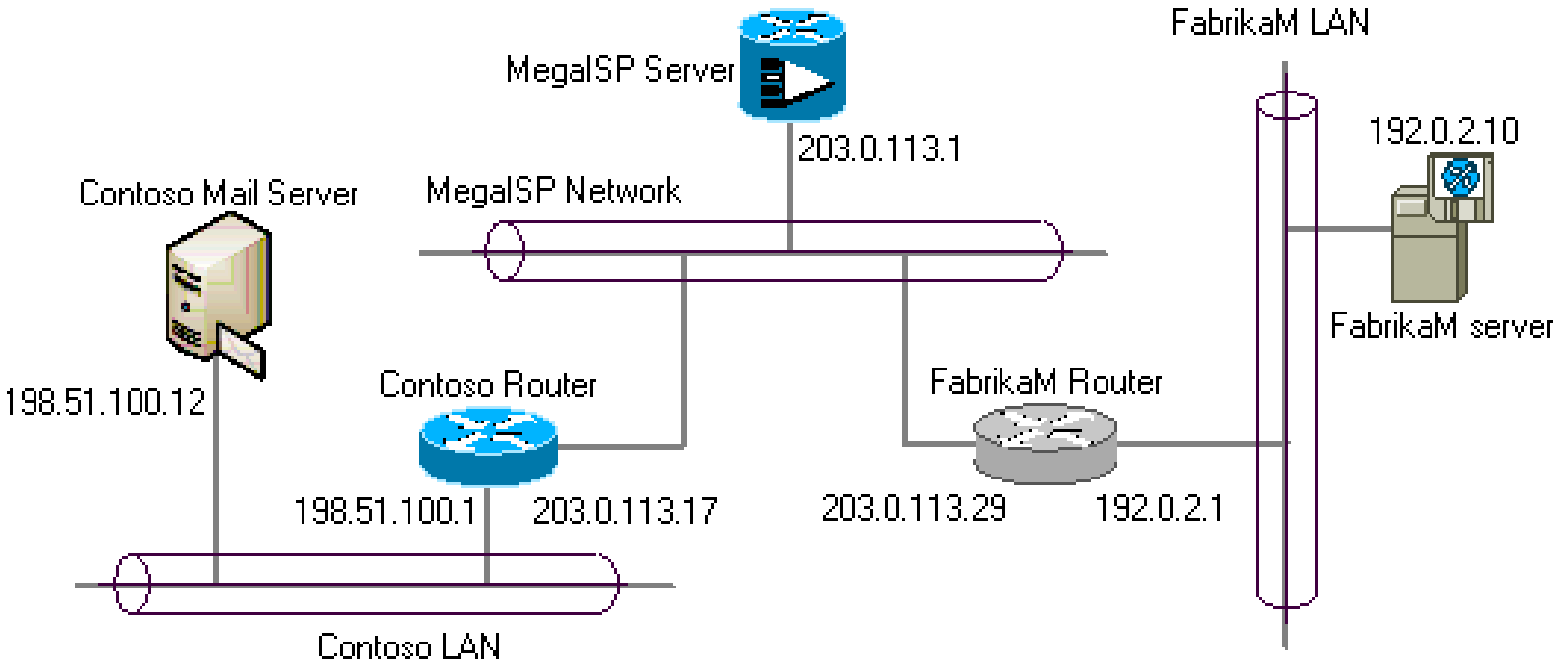
- Povezaćemo se na Web server, čime simuliramo pristup unutrašnjem mrežnom servisu (npr. Sharepoint Portal)



IPSec kao zaštita za druge vrste tunela

Puštamo tunel bez šifrovanja

- Povezali smo se preko nekog tunela koji nema šifrovanje (IP-IP)
- Ovo možemo da koristimo i kada želimo automatski prelaz na drugi link

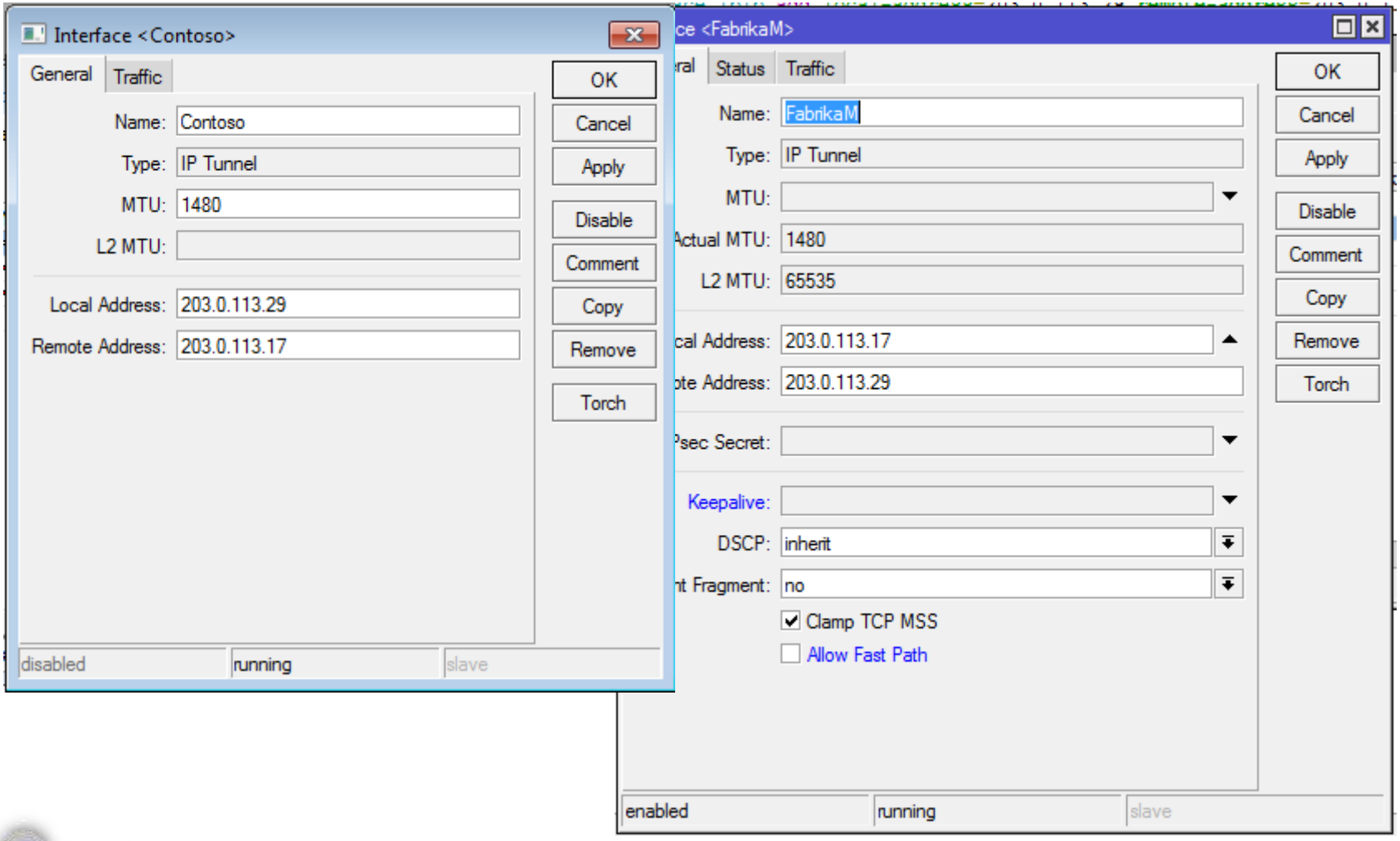


Šta nam je cilj?

- Pravimo tunel koji nema šifrovanje, ali može da se rutira, između dve tačke na Internetu.
- Treba da uradimo sledeće korake:
  - dodajemo novi virtuelni interfejs IP-tunel,
  - dodelimo mu adresu
  - postavljamo statičku rutu ka udaljenoj mreži
  - podešavamo IPSec u transport režimu

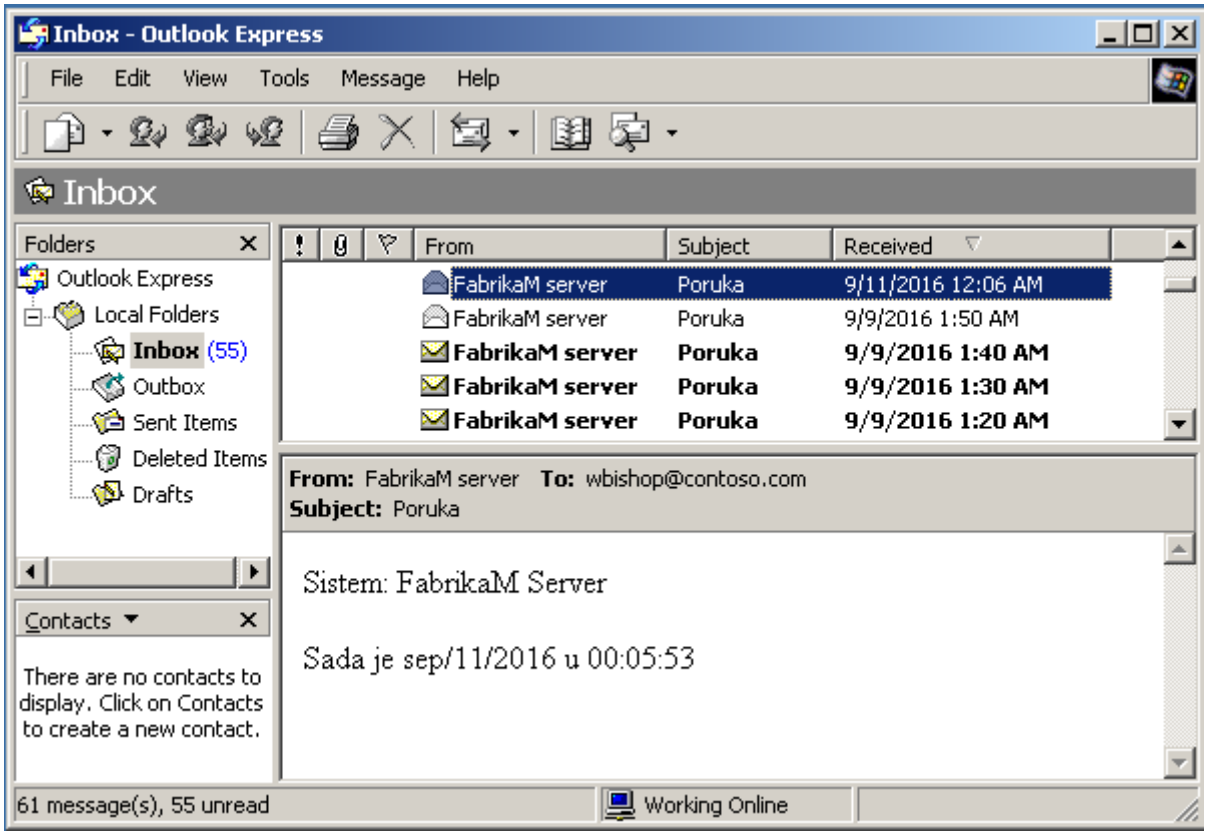
Podešavamo IP-IP tunel

- Podesićemo IP tunel na obe strane



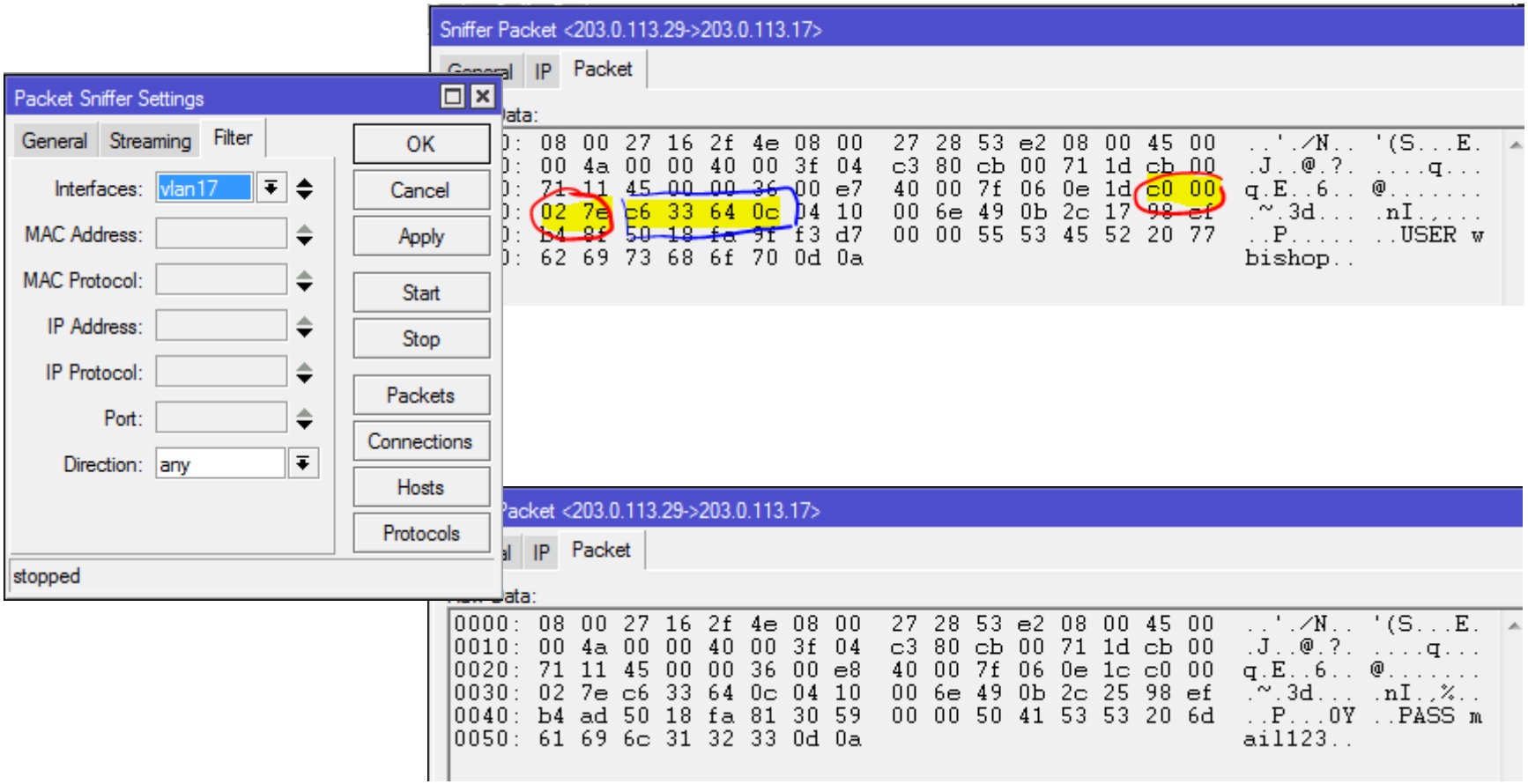
Testiramo tunel

- Ukoliko je sve dobro podešeno, tunel se podigao i komunikacija se obavlja nesmetano



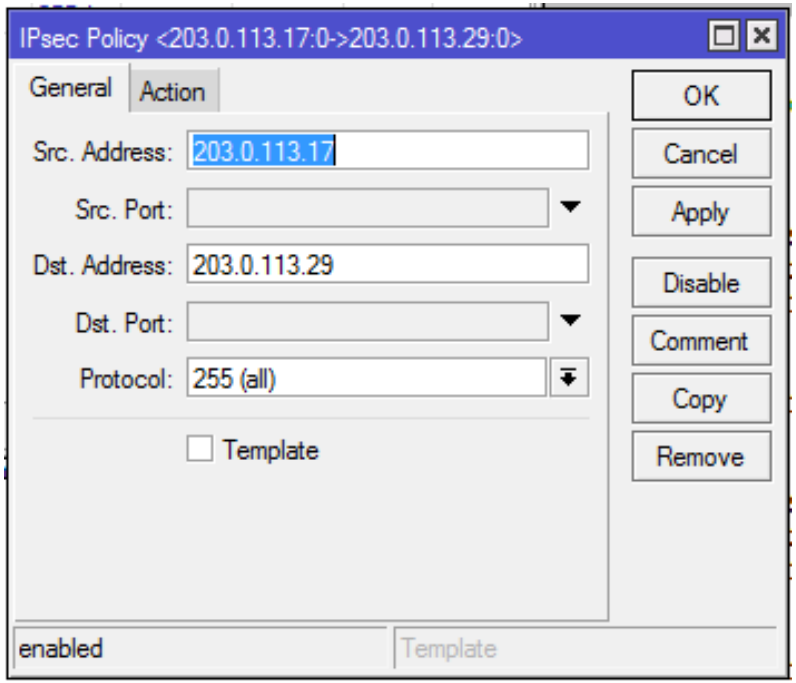
Saobraćaj je nezaštićen

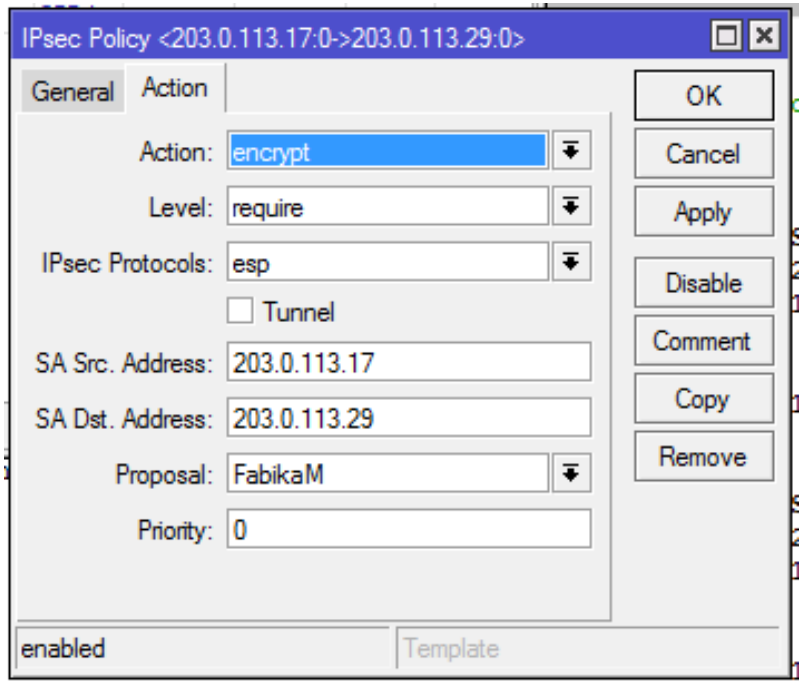
- Pustili smo packet sniffer na MegaISP ruteru i uhvatili saobraćaj



Dodajemo IPSec zaštitu

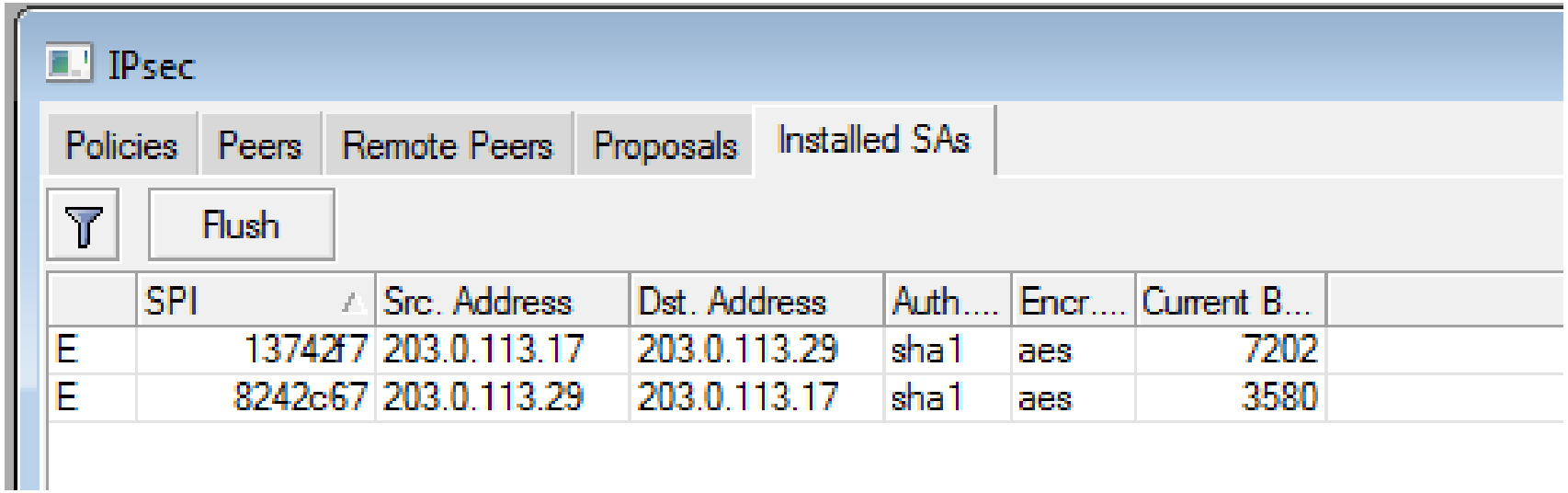
- Pravimo IPSec tunel u **transport** režimu
- Tunel se pravi između javnih adresa oba rutera
- U ovom režimu se mogu koristiti samo host adrese (/32)





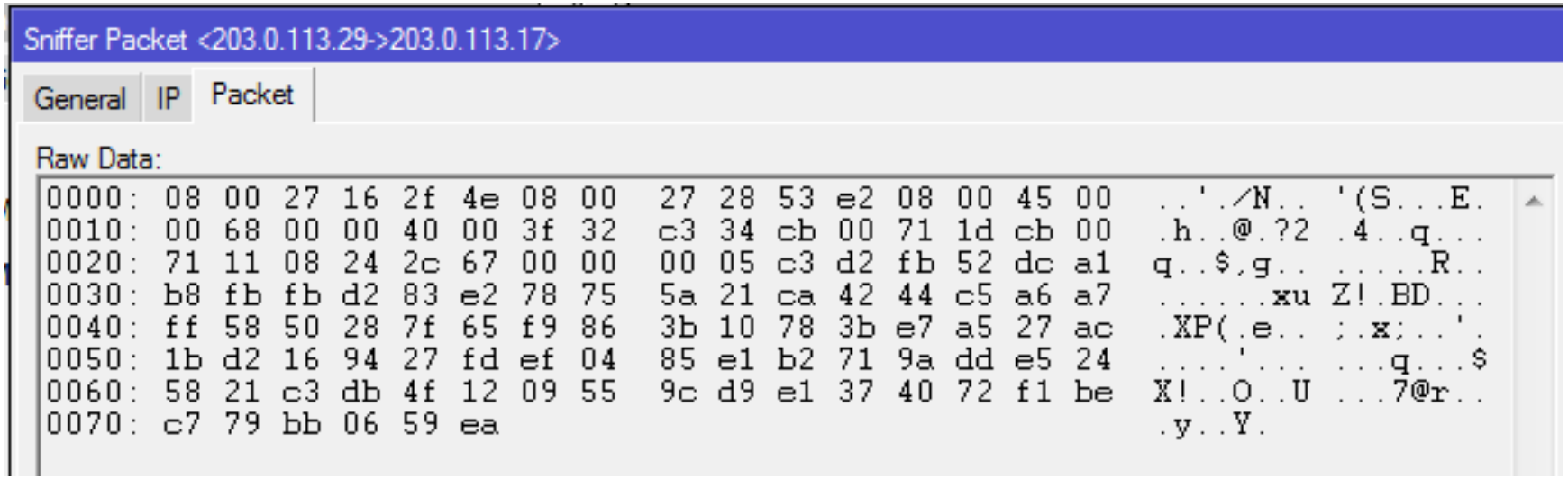
IPSec se uspostavio

- IPSec će se uspostaviti čim krene saobraćaj



Saobraćaj je zaštićen od prisluškivanja

- Na MegaISP ruteru više ne možemo da uhvatimo detalje saobraćaja

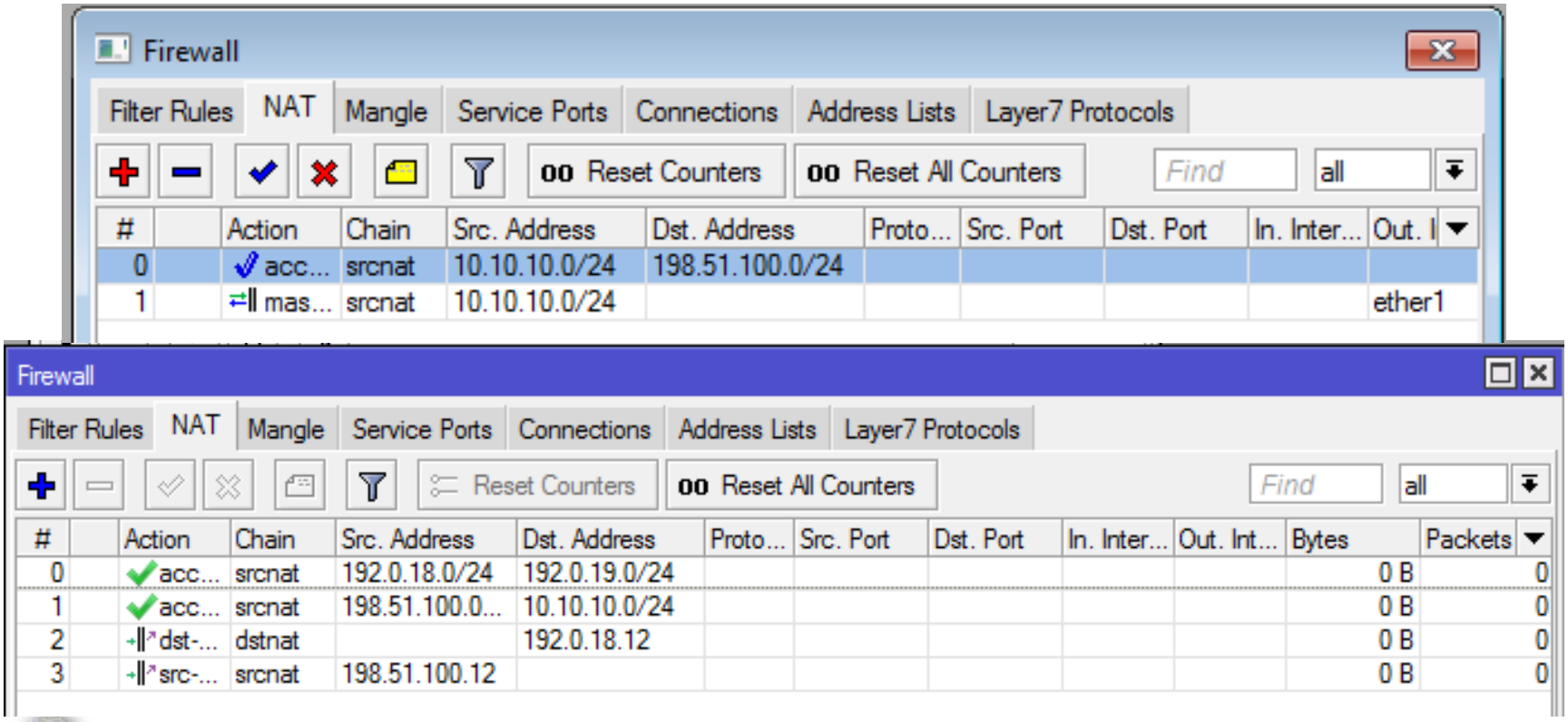


Demo

Rešavanje problema

Zaobilaženje izlaznog NAT-a

- IPSec saobraćaj mora da ode u tunel
- Potrebno je da se izuzme od izlaznog NAT-a
- Ova pravila moraju da budu na vrhu liste



Ukoliko se ne uspostavlja faza I

- Proverite da li u dnevniku događaja imate ovakve redove

```
22:37:37 ipsec,debug,packet 76 bytes from 203.0.113.17[500] to 203.0.113.29[500]
22:37:37 ipsec,debug,packet sockname 203.0.113.17[500]
22:37:37 ipsec,debug,packet send packet from 203.0.113.17[500]
22:37:37 ipsec,debug,packet send packet to 203.0.113.29[500]
22:37:37 ipsec,debug,packet src4 203.0.113.17[500]
22:37:37 ipsec,debug,packet dst4 203.0.113.29[500]
22:37:37 ipsec,debug,packet 1 times of 76 bytes message will be sent to
203.0.113.29[500]
```

- Ako se pojavi promena porta na 4500, a ni jedan od rutera nije iza NAT-a, onda jedna strana ne aktivira pravo IKE I pravilo
- Ukoliko imate više Internet linkova na istom ruteru, postavite statičku rutu ka drugoj strani u `ip routes`

Ukoliko nema razmene saobraćaja kroz tunel

- Ukoliko se desi da se saobraćaj ne razmenjuje, uključićemo dnevnik događaja za IPSec protokol
- Ukoliko hvatamo događaje u memoriju, povećaćemo memorijski dnevnik na bar 1000 linija
- Najbolje je snimiti događaje na disk ili poslati na SysLog
- Obratite pažnju da li postoji ovakav deo u dnevniku događaja

Sep/08/2016 22:39:03	memory	ipsec, debug, packet	get a src address from ID payload 192.0.2.0[0] prefixlen=24 ul_proto=255
Sep/08/2016 22:39:03	memory	ipsec, debug, packet	get dst address from ID payload 198.51.100.0[0] prefixlen=24 ul_proto=255
Sep/08/2016 22:39:03	memory	ipsec, debug, packet	suitable SP found:198.51.100.0/24[0] 192.0.2.0/24[0] proto=any dir=out
Sep/08/2016 22:39:03	memory	ipsec, debug, packet	(proto_id=ESP spisize=4 spi=00000000 spi_p=00000000 encmode=Tunnel reqid=1:1)
Sep/08/2016 22:39:03	memory	ipsec, debug, packet	(tms_id=AES-CBC encklen=256 authtype=hmac-sha1)
Sep/08/2016 22:39:03	memory	ipsec, debug, packet	total SA len=52

Neke značajnije poruke u dnevniku

- U slučaju problema uvek pogledajte dnevnik događaja za IPSec

```
15:10:41 ipsec IPsec-SA request for 203.0.113.17 queued due to no phase1 found.
15:10:41 ipsec initiate new phase 1 negotiation: 192.168.1.2[500]<=>203.0.113.17[500]
15:10:41 ipsec begin Identity Protection mode.
. . .
15:10:43 ipsec NAT detected: ME
15:10:43 ipsec KA list add: 192.168.1.2[4500]->203.0.113.17[4500]
15:10:43 ipsec ISAKMP-SA established 192.168.1.2[4500]-203.0.113.17[4500]
spi:18a2d5a3ff1490d1:ee323f57fb46ae25
15:11:12 ipsec initiate new phase 2 negotiation: 192.168.1.2[4500]<=>203.0.113.17[4500]
15:11:12 ipsec NAT detected -> UDP encapsulation (ENC_MODE 1->3).
15:11:13 ipsec phase2 negotiation failed due to time up waiting for phase1. ESP
203.0.113.17[500]->192.168.1.2[500]
15:11:13 ipsec delete phase 2 handler.
15:11:13 ipsec fatal NO-PROPOSAL-CHOSEN notify messsage, phase1 should be deleted.
. . .
15:17:56 ipsec Adjusting my encmode UDP-Tunnel->Tunnel
15:17:56 ipsec Adjusting peer's encmode UDP-Tunnel(3)->Tunnel(1)
15:17:56 ipsec IPsec-SA established: ESP/Tunnel 203.0.113.17[4500]->192.168.1.2[4500]
spi=160904474(0x997351a)
15:17:56 ipsec IPsec-SA established: ESP/Tunnel 192.168.1.2[4500]->203.0.113.17[4500]
spi=138579378(0x8428db2)
```

Zaključak

Pričali smo o ovome

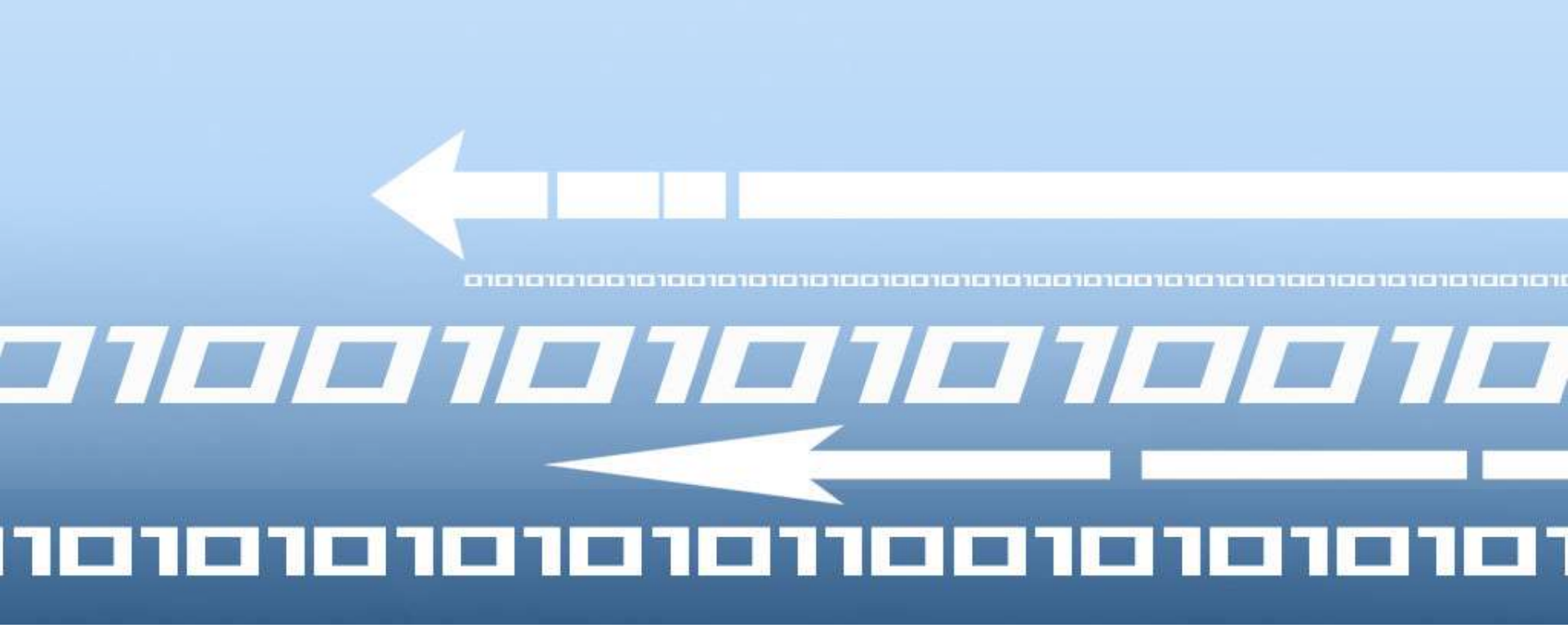
- Govorili smo o IPSec servisima
- Napravite dokument sa parametrima za obe strane
- Pokazali smo kako se pravi site-to-site IPSec tunel
- Pokazali smo kako se pravi IPSec tunel kroz NAT
- Pokazali smo kako se pravi L2TP/IPSec tunel za udaljene korisnike
- Pokazali smo kako se pravi IPSec tunel za zaštitu tunela bez šifrovanja
- Šta proveriti ukoliko imamo problem u komunikaciji?

Šta dalje?

- Konsultujte uputstva proizviđača
- Pogledajte Mikrotik Wiki za više informacija i studije slučaja
- Pratite moj blog https://mivilisnet.wordpress.com/
- Kontaktirajte predavača preko e-pošte:

sstanisic@algotech.rs

s.stanisic@hotmail.com



Hvala na pažnji !!!