Mikrotik Muito além dos ISPs

Por: Marcos Velez

Redes Brasil

O mercado de TI

Com a crescente busca por novas soluções, seja com custo melhor, ou por algumas funcionalidades não disponíveis em outras soluções, algumas corporações vem gradativamente adotando as soluções Mikrotik.

Assim, em alguns grupos de lojas, toda a solução para comunicação entre matriz-filial foi adotada a solução 100% MikroTik.

Alguns clientes ainda desconfiados já que todos os equipamentos comprados não custaram nem 1/3 da solução mais barata, resolveram “apostar”.

Existe ainda um mercado inexplorado por nós, com o RouterOS é possível vendermos vpns, por exempo utilizando nossa rede.

Redes Brasil

Alguns Cases de Sucesso

- REDE DE COSMÉTICOS

Necessidade Inicial: Configurar uma RouterBoard em uma filial com um link IP, para fechar um túnel IPSEC entre a filial e a matriz, que utilizava FORTINET.

E foi aberta uma nova loja... Outra loja... outra... E outra...

E proporcionalmente aumentando e mudando as necessidades.

Redes Brasil

Cases de sucesso

Daí eis que surgem novas necessidades:

- Colocar um segundo link ip para prover redundância na filial...
- Autenticar usuários remotos em seus smartphones para acessar o sistema local...
- Trocar o equipamento da matriz por uma RouterBoard por conta do processamento elevado da outra solução
- Configurar o sistema de alta disponibilidade na matriz para que se um roteador pare o outro assuma.
- Adotar uma solução mais compatível com os provedores locais, porque em alguns provedores não era possível ter conectividade fim-a-fim verdadeira, pré requisito do IPSEC.
- ETC..

Redes Brasil

Cases de sucesso

- REDE DE MAGAZINE

Necessidade inicial: Configurar uma RB para utilizar um link IP instalado para fechar VPN Ipsec entre matriz e filial, utilizando-o como link principal, e mantendo um link secundário MPLS da operadora. Para tratamento da disponibilidade, utilizamos um Túnel GRE para tratamento do status da pseudo-interface.

Outras necessidades: Realizar a checagem do link secundário enviando e-mail caso o link caísse.

Redes Brasil

Cases de sucesso

- REDE DE LOJAS DE ELETRONICOS

Necessidade inicial: Criar um servidor PPTP para a direção trabalhar remotamente.

A ferramenta mostrou-se tão versátil que hoje além de atuar como roteador, firewall, as routerboards também são responsável pela rede wireless, QoS e por fim a interligações (VPN) entre matriz e filiais.

Redes Brasil

Cases de sucesso

- REDE DE SUPERMERCADOS

Necessidade inicial: Instalar uma rede wireless outdoor (utilizando QRT) para interligar 3 de suas lojas que estavam fisicamente próximas.

Após essa rede outdoor, interligamos as filiais por meio de túneis que possibilitam tunelamento e serem postas na bridge.

Redes Brasil

Cases de sucesso

- EMPRESA TRANSPORTE URBANO

Necessidade inicial: Fazer um balanceamento com failover para usar dois links instalados.

Após essa configuração, também foi integrado o sistema de VPN OPENVPN com outra empresa, com a finalidade de compartilhar o rastreamento da frota. Depois surgiu a necessidade um LAN2LAN com outra garagem, utilizando um ip

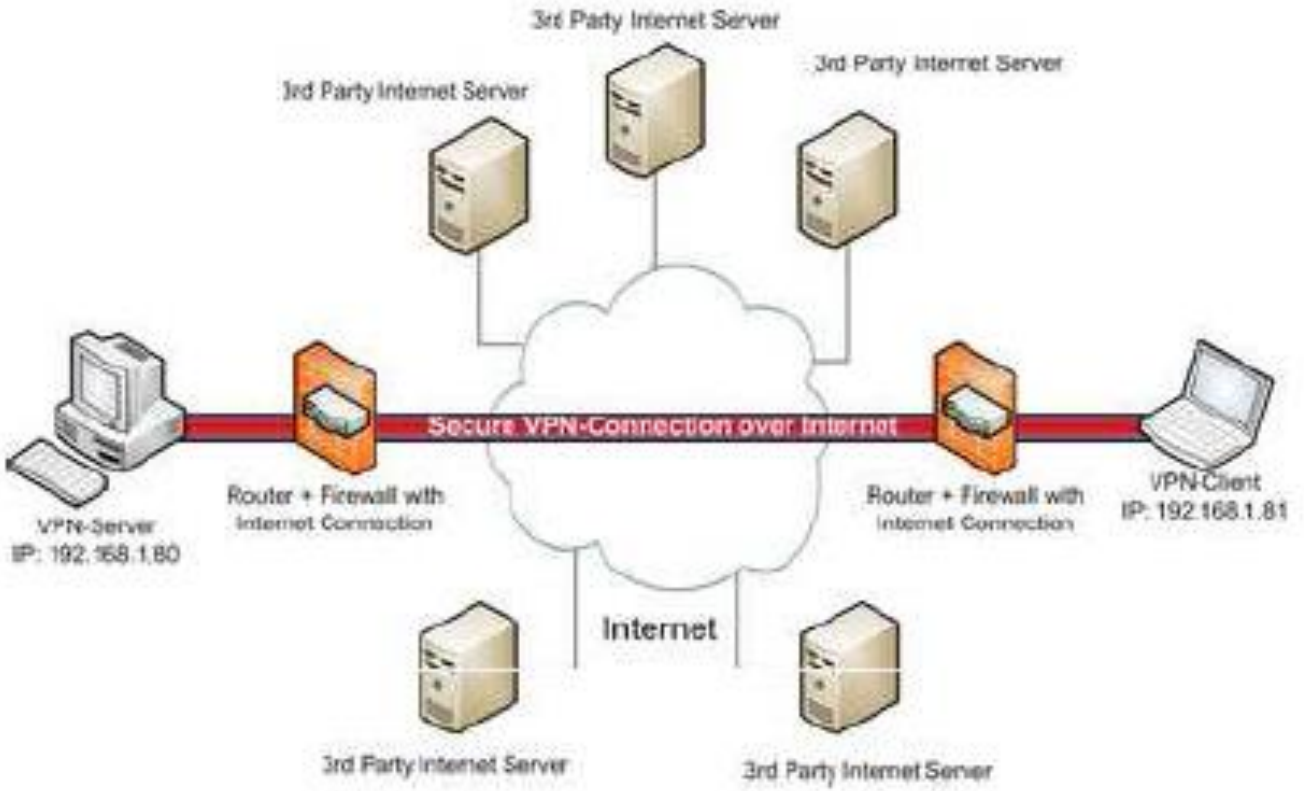
Redes Brasil

O QUE É UMA VPN

- Uma Rede Privada Virtual é uma rede de comunicações privada normalmente utilizada por uma empresa ou conjunto de empresas e/ou instituições, construídas em cima de uma rede pública.
- VPNs podem ser seguras se usados protocolos de criptografia por tunelamento que fornecem confidencialidade, autenticação e integridade necessárias para garantir a privacidade dos dados.

Redes Brasil

Exemplo de VPN



Redes Brasil

VPN

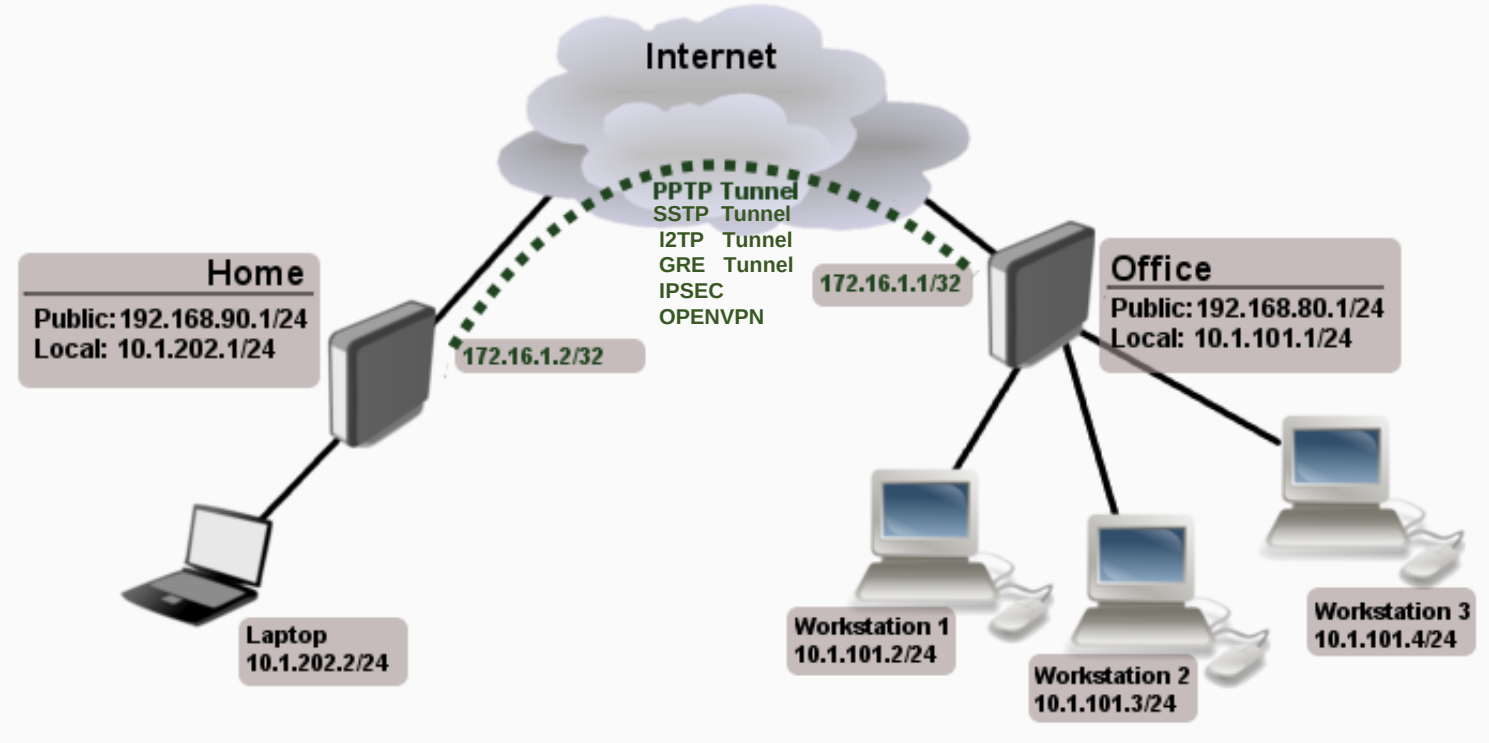
- As principais características da VPN são:
  – Promover acesso “seguro” sobre meios físicos públicos como a internet por exemplo.
  – Promover acesso seguro a serviços em ambiente corporativo de e-mail, impressoras, etc...
  – Fazer com que o usuário, na prática, se torne parte da rede corporativa remota recebendo IPs desta e perfis de segurança definidos.
  – A base da formação das VPNs é o tunelamento entre dois pontos, porém tunelamento não é sinônimo de VPN.

Tunelamento

- Por definição de tunelamento, é a capacidade de criar túneis entre dois hosts por onde trafegam dados, assim com na engenharia civil, o túnel é um meio de “encurtar o caminho” tornando desprezível o conteúdo que trafega por “cima”.
- O Mikrotik implementa diversos tipos de tunelamento, podendo ser tanto servidor como cliente desses protocolos:
  - PPP (Protocolo de Ponto Ponto)
  - PPPoE (Protocolo de Túneis Ponto a Ponto sobre Ethernet)
  - PPTP (Protocolo de Tunelamento Ponto a Ponto)
  - L2TP (Protocolo de Tunelamento de camada 2)
  - OVPN (Open Virtual Private Network)
  - IPSec (IP Security)
  - Túneis IPIP (Encapsula pacotes IP em pacotes IP)
  - Túneis VPLS (Serviço de LAN Privada Virtual)
  - Túneis TE (Túneis de Engenharia de Tráfego)
  - Túneis GRE (Encapsulamento de Roteamento Genérico
  - Túneis EoIP (Ethernet sobre IP, proprietário Mikrotik)
  - Túneis SSTP (Protocolo de encapsulamento de Ligação Segura)

Tipos de Configurações de VPN

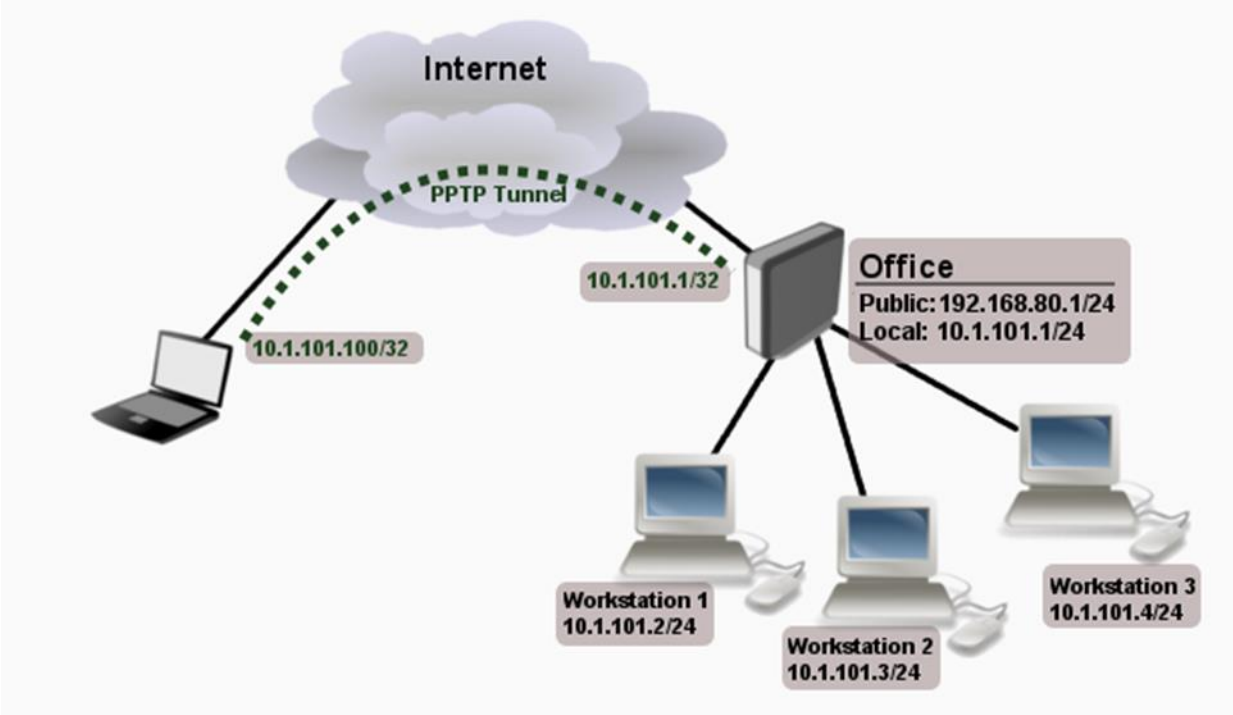
- VPN SITE TO SITE (conexão de duas redes lan por roteadores)



Redes Brasil

Tipos de configurações de VPN

- VPN SITE TO CLIENT (Conexão Remota entre o dispositivo e o roteador)



Redes Brasil

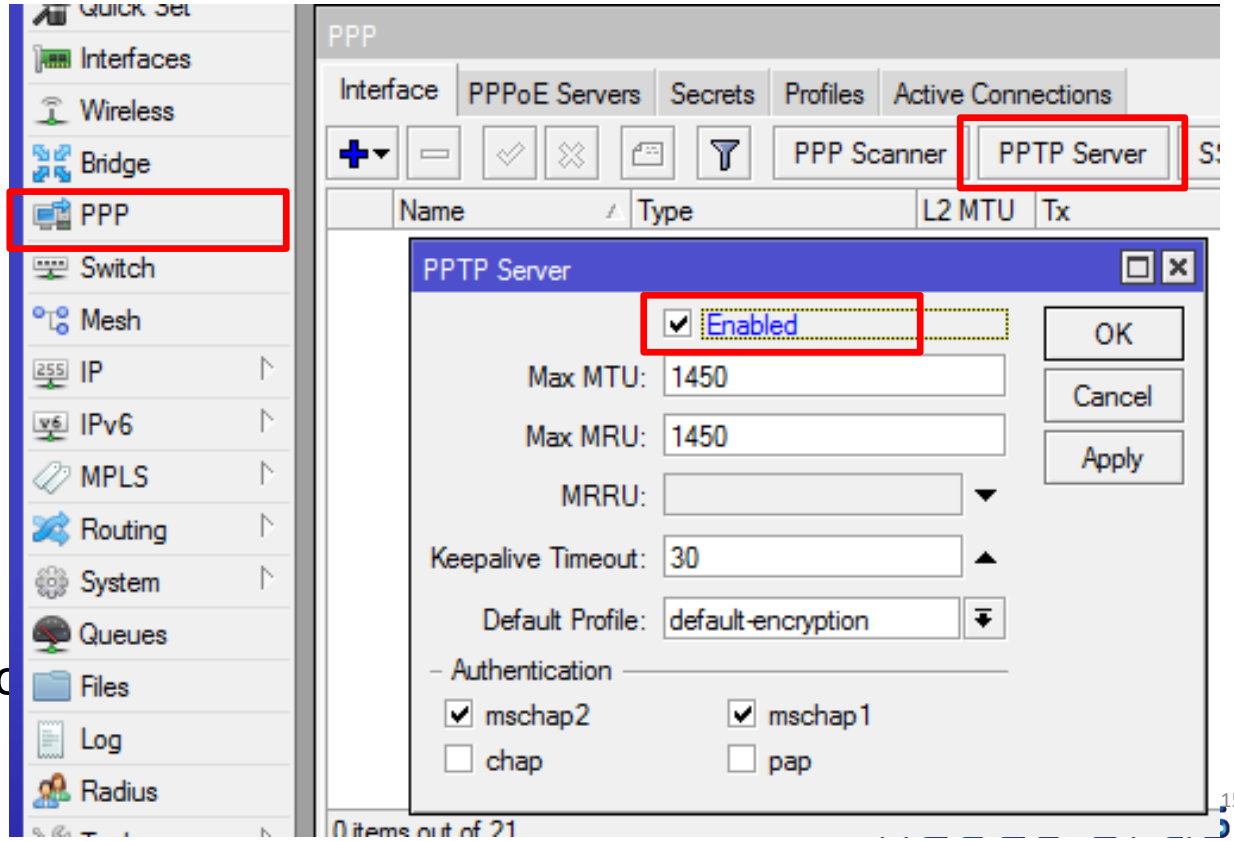
Como configurar?

- A configuração de túneis mais simples, e consequentemente mais compatível é o PPTP, lembrando que simplicidade geralmente não é sinônimo de segurança.

NO MIKROTIK...

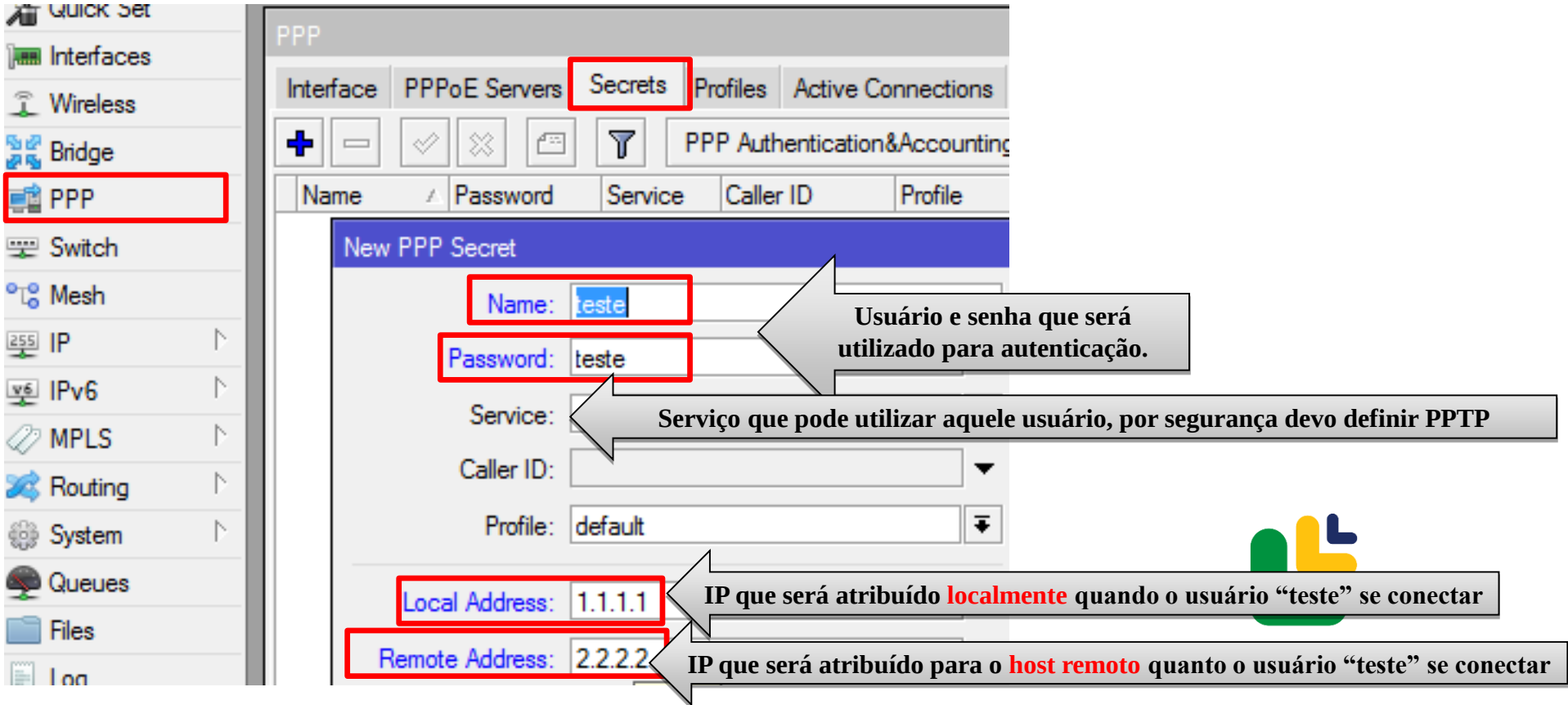
São apenas 2 passos.

Ativar o servidor em um roteador que obviamente seja alcançável pelos outros dispositivos.
Ex.com ip publico



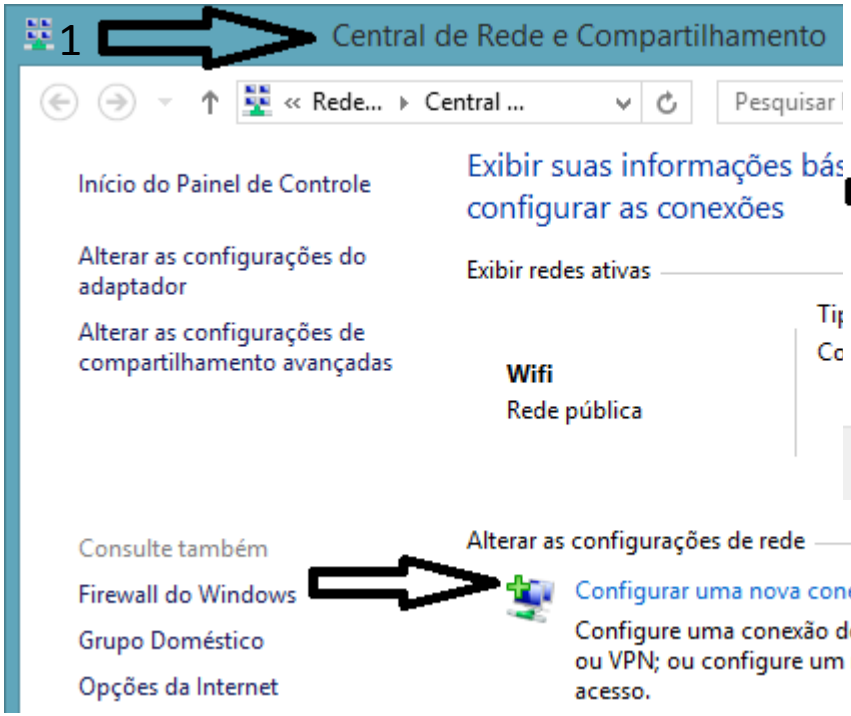
Como configurar?

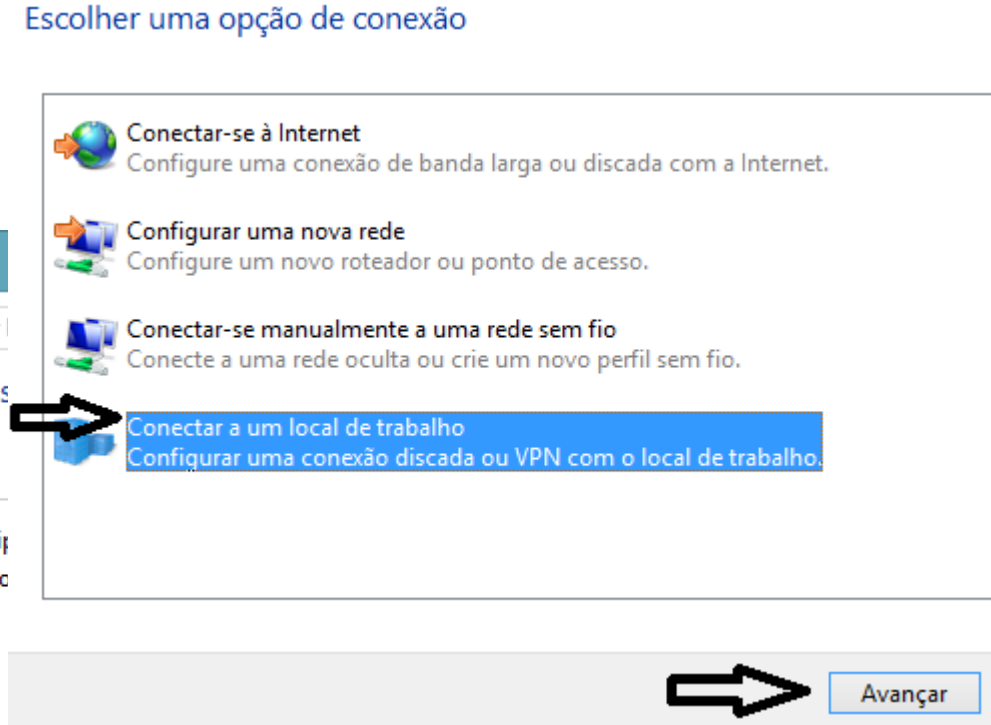
O Segundo passo é criar os usuários que irão se autenticar neste roteador. Lembrando que o Ips Locais e Remotos se fazem necessários apenas se não configurados no Perfil.



Como configurar conexão PPTP Cliente

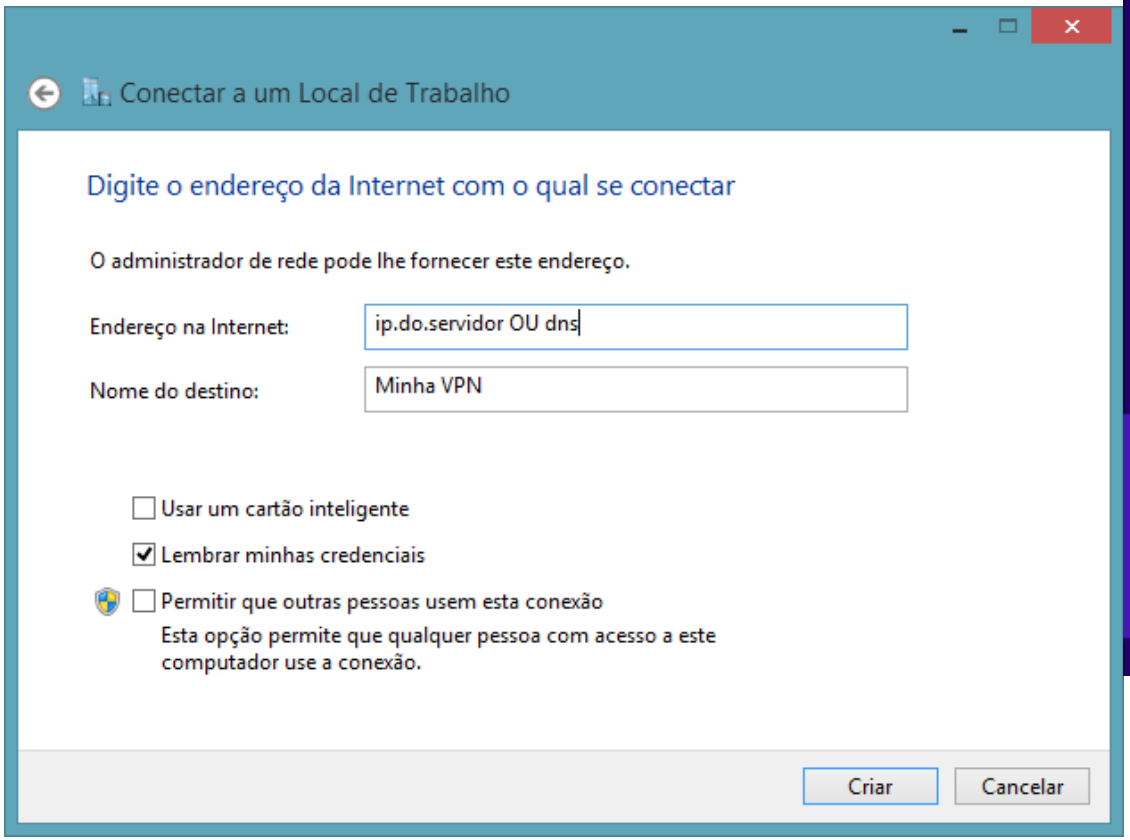
- NO PC WINDOWS 7,8

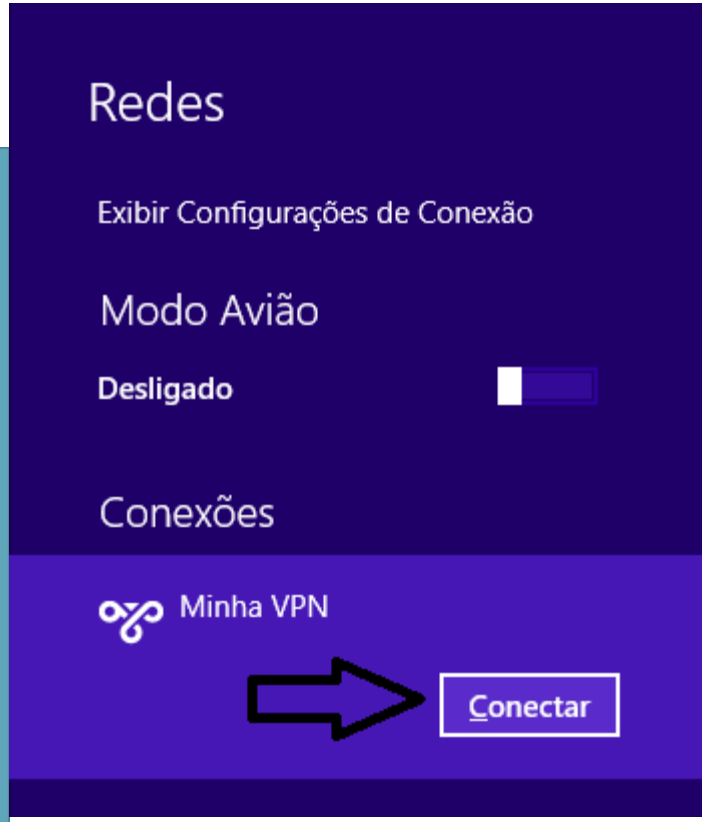




Como configurar conexão PPTP Cliente

- NO WINDOWS

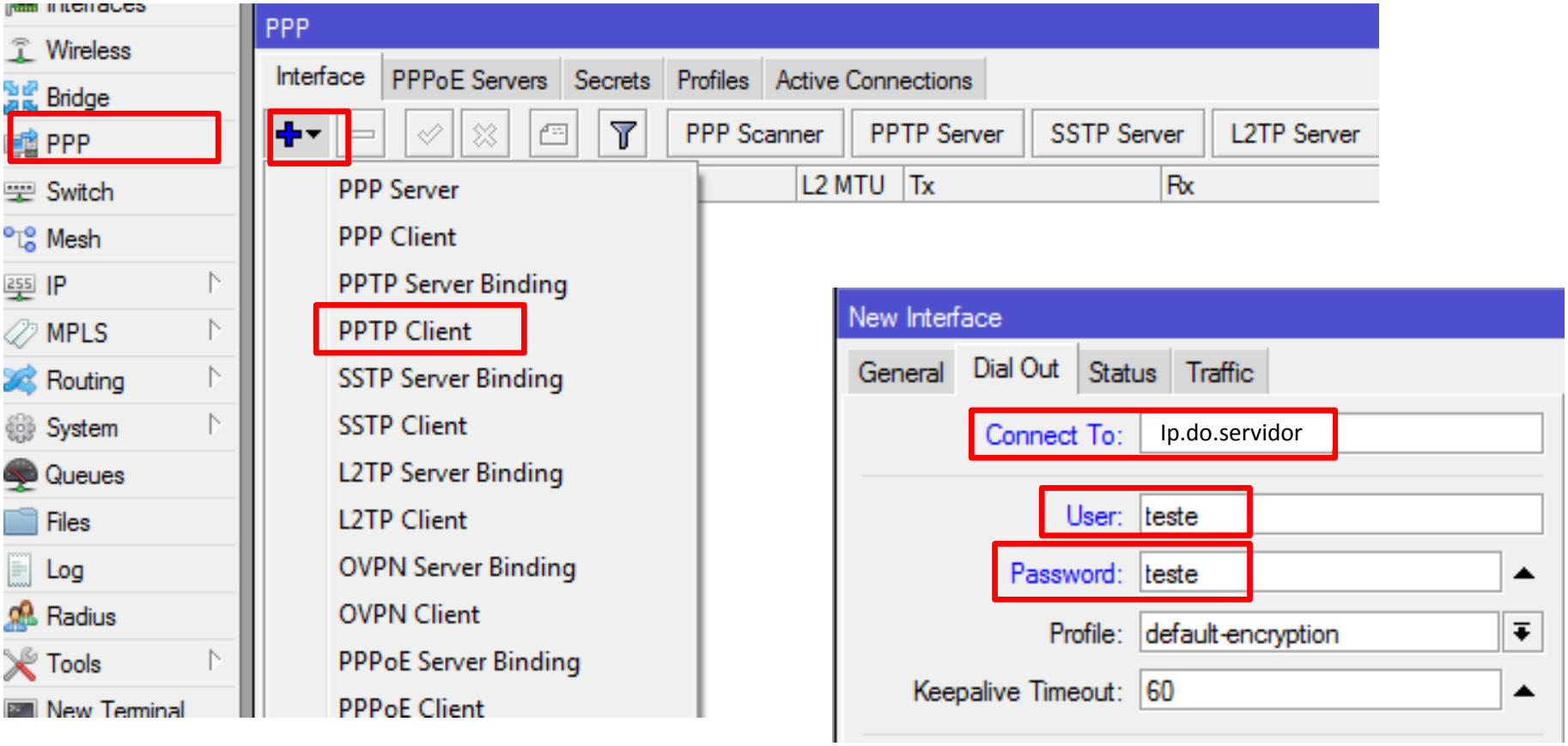




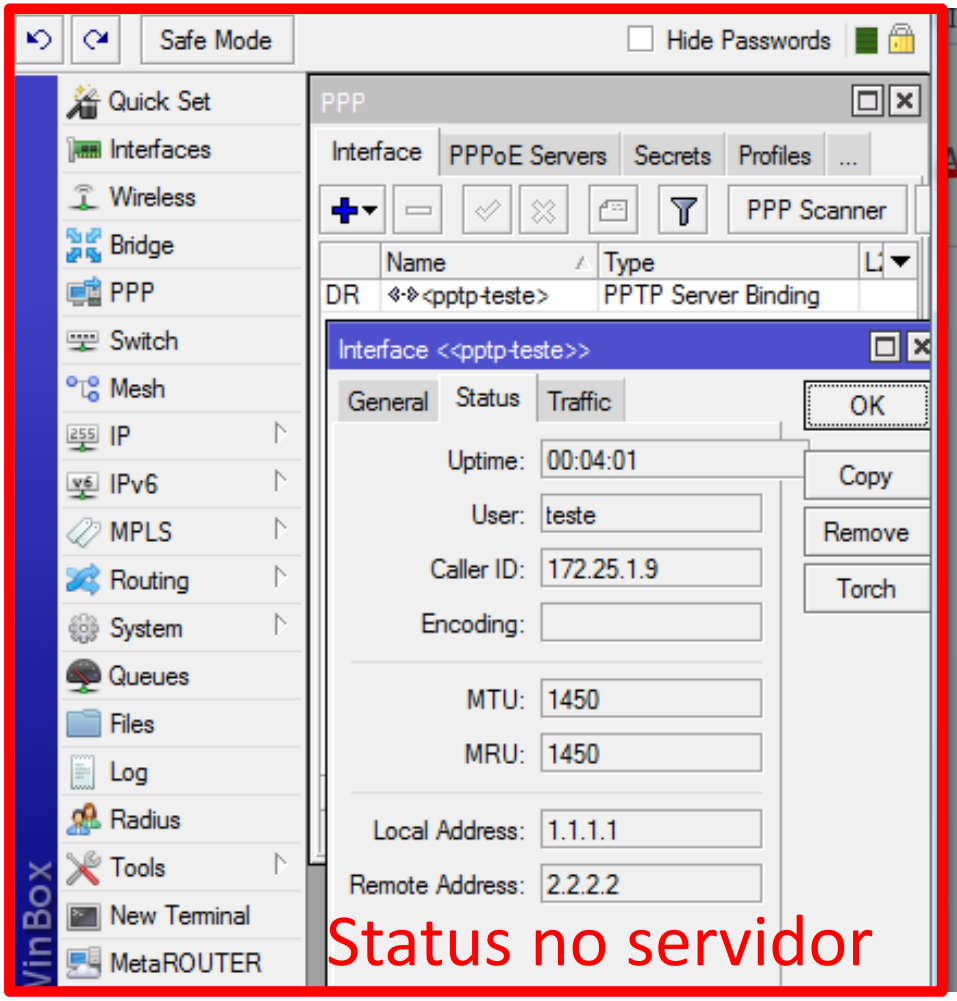
Redes Brasil

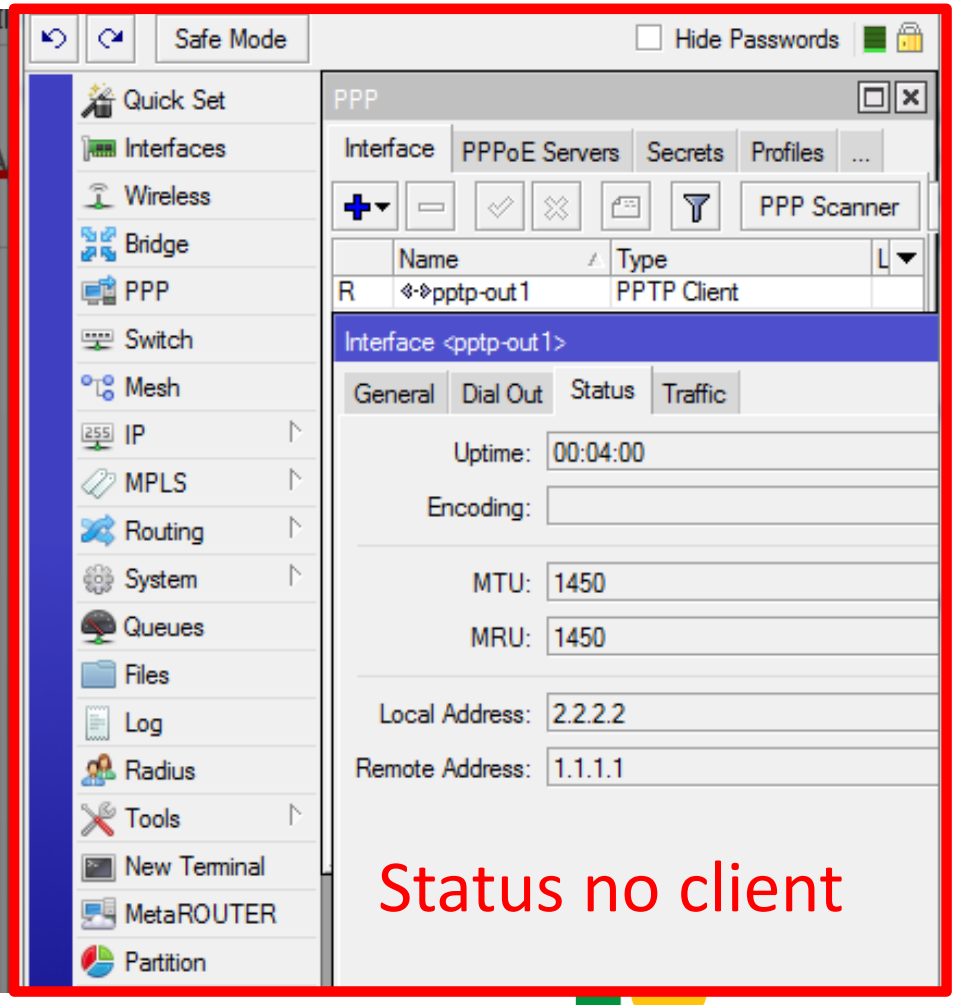
Como configurar conexão PPTP Cliente

- NO MIKROTIK ROUTEROS



Como saber o status da conexão

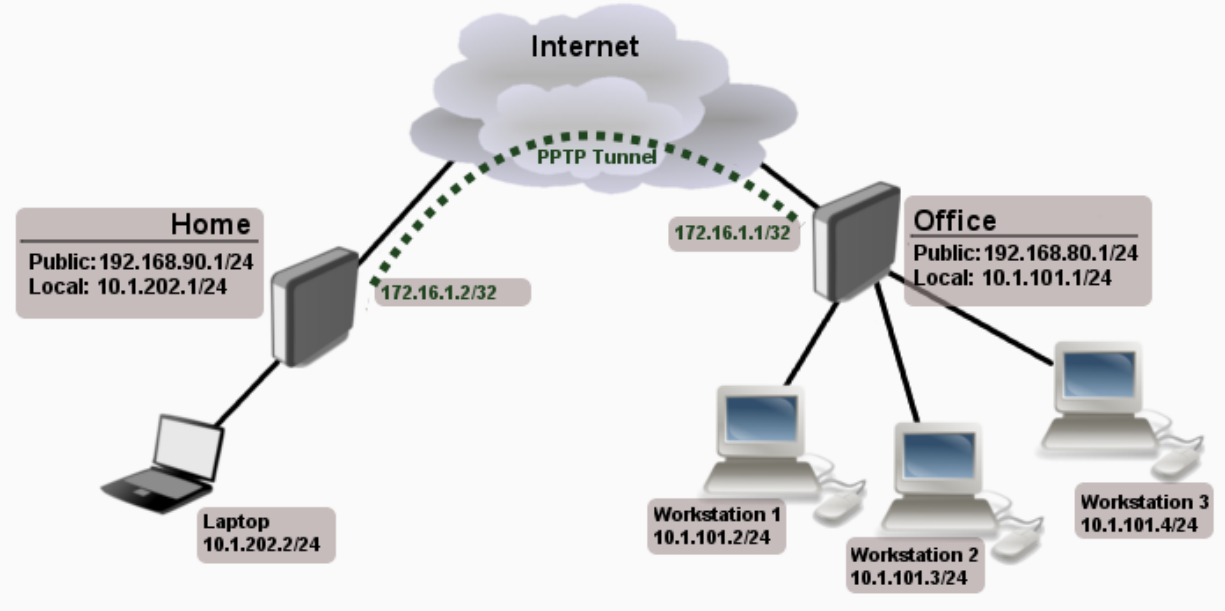


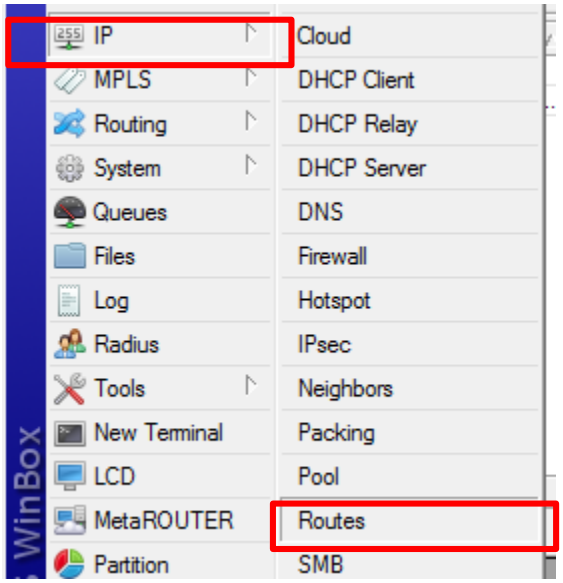


Redes Brasil

E se for uma conexão site to site é só isso?

- Não! Precisaremos ainda configurar as rotas, seja criando rotas estáticas ou podemos utilizar algum protocolo de roteamento dinâmico.

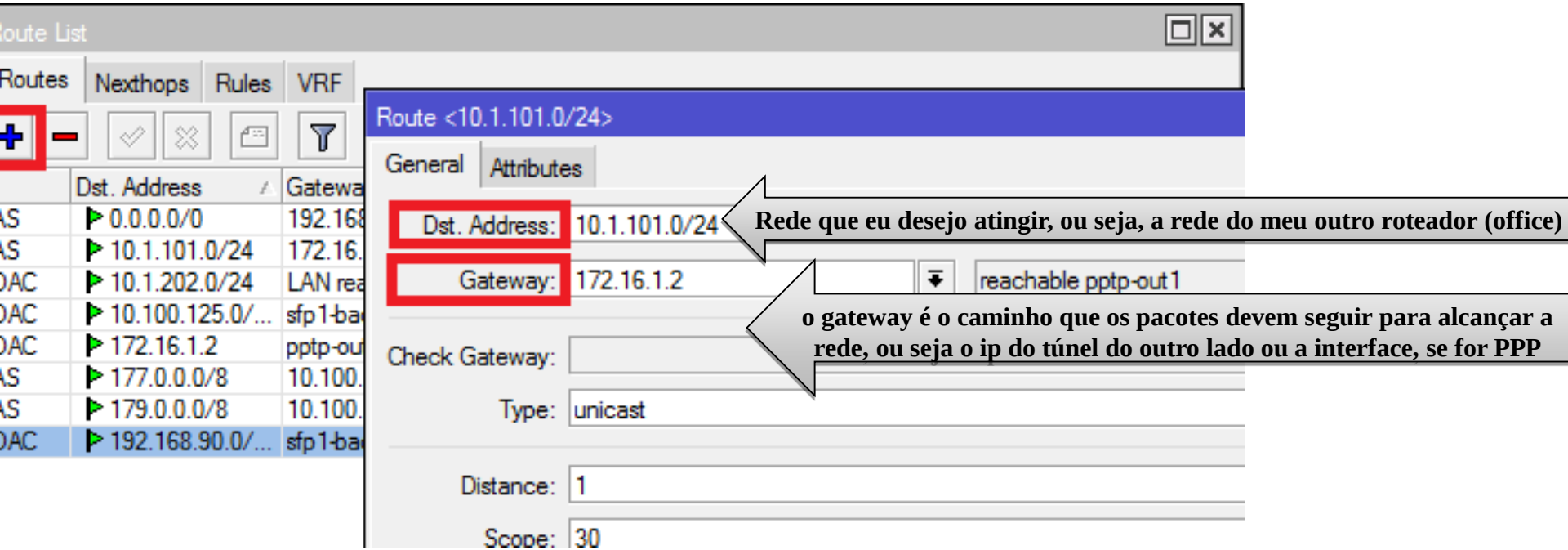




Redes Brasil

Criando as rotas conforme o cenário anterior

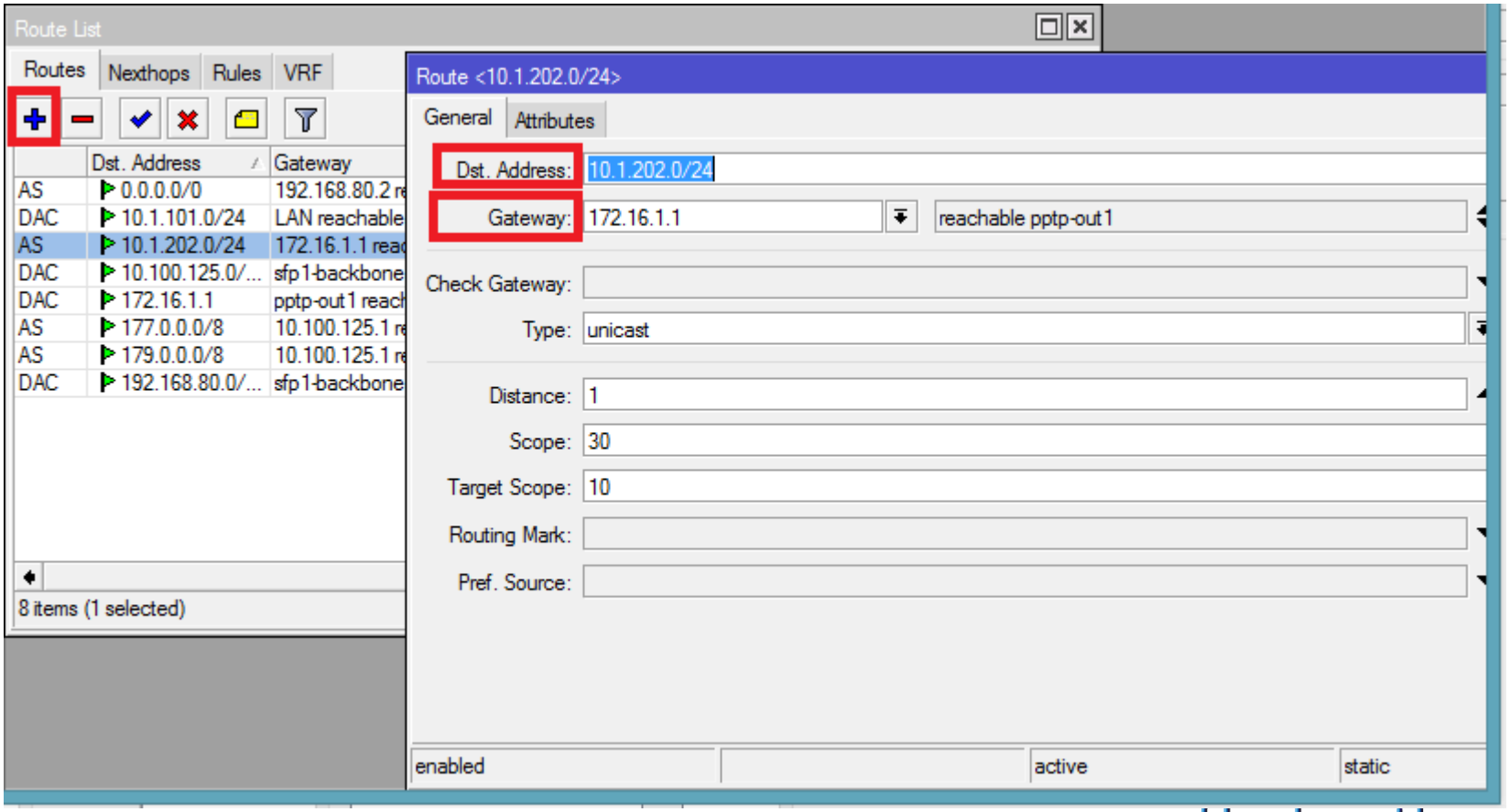
- No roteador Home



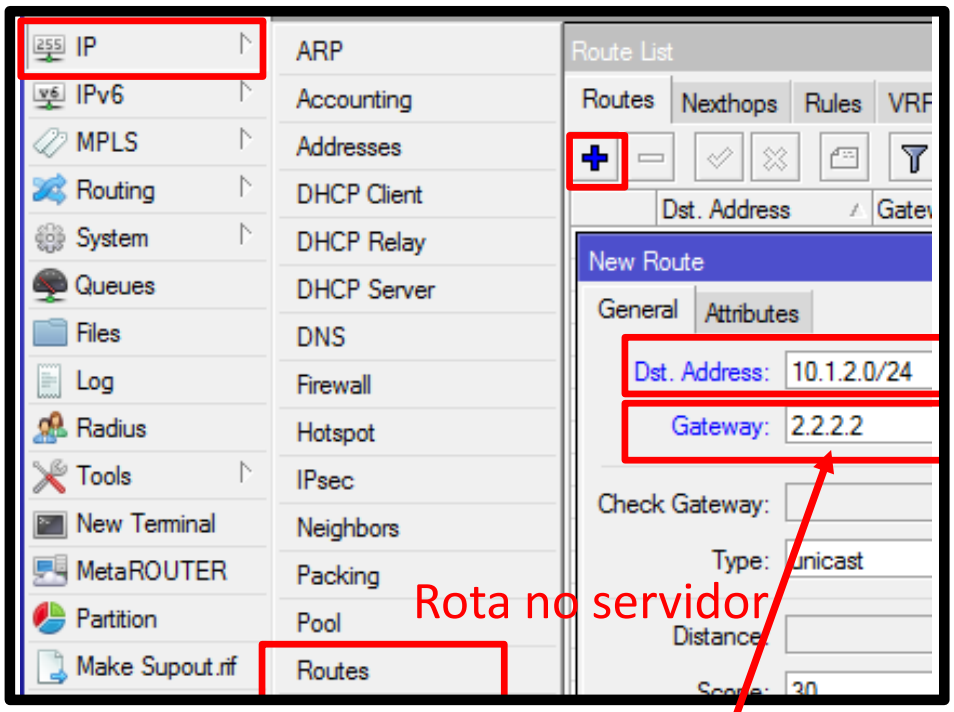
Redes Brasil

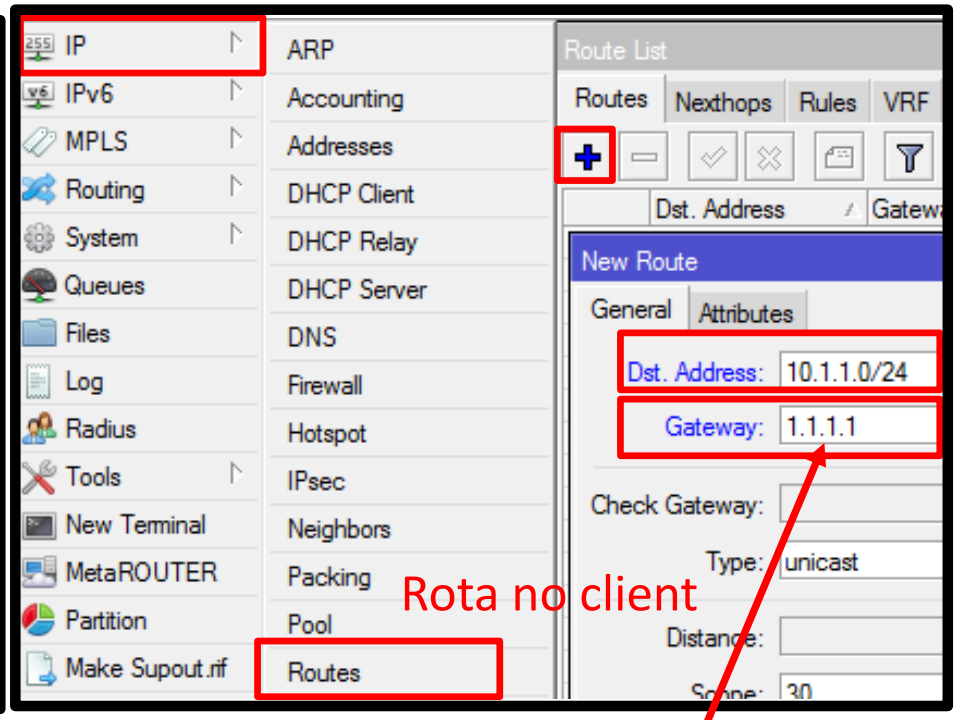
Criando as rotas conforme o cenário anterior

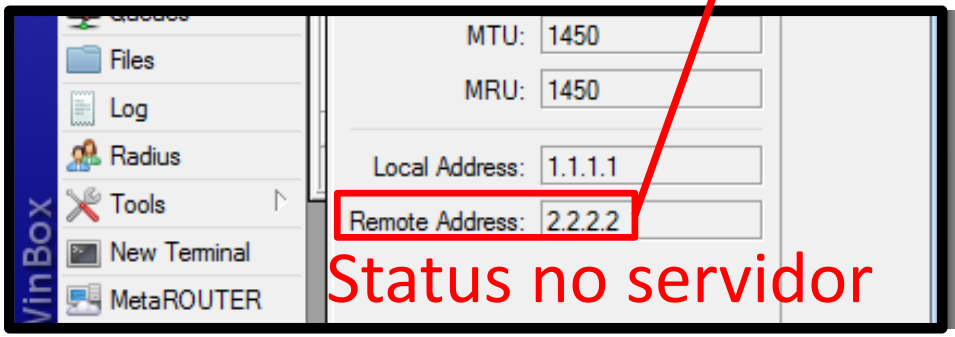
- No roteador OFFICE

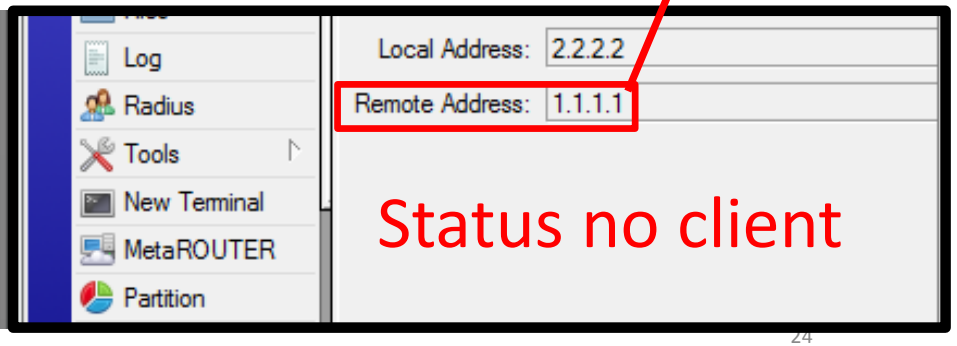


Outro exemplo (criando as rotas)









PPP – Definições Comuns para os serviços

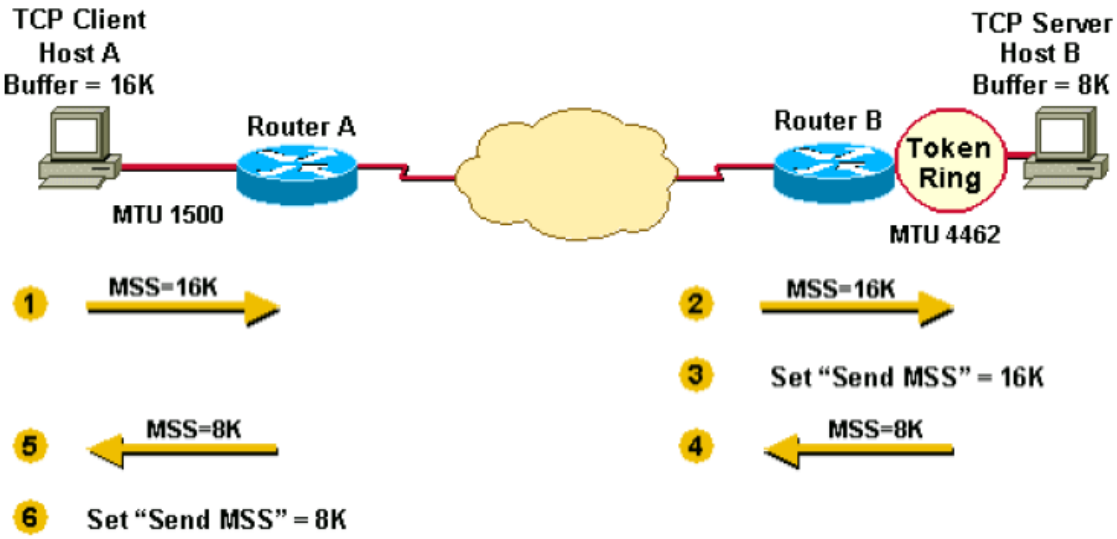
- **MTU/MRU**: Unidade máximas de transmissão/ recepção em bytes. Normalmente o padrão ethernet permite 1500 bytes.

Em serviços PPP que precisam encapsular os pacotes, deve-se definir valores menores para evitar fragmentação.

- **Keepalive Timeout**: Define o período de tempo em segundos após o qual o roteador começa a mandar pacotes de keepalive por segundo. Se nenhuma reposta é recebida pelo período de 2 vezes o definido em keepalive timeout o cliente é considerado desconectado.
- **MRRU**: Tamanho máximo do pacote, em bytes, que poderá ser recebido pelo link.
- **Authentication**: As formas de autenticação permitidas são:
  - **Pap**: Usuário e senha em texto plano sem criptografica.
  - **Chap**: Usuário e senha com criptografia.
  - **Mschap1**: Versão chap da Microsoft conf. RFC 2433
  - **Mschap2**: Versão chap da Microsoft conf. RFC 2759

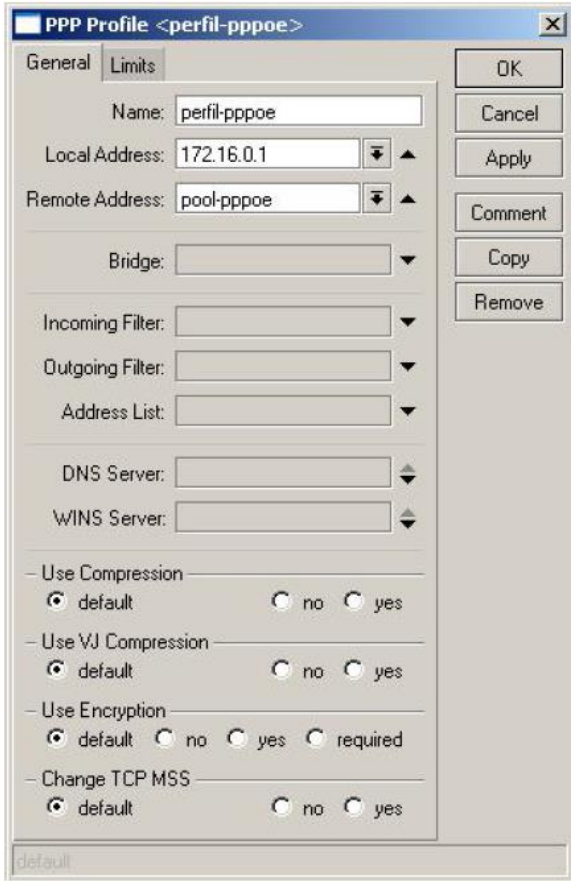
PPP – Definições Comuns para os serviços

Change MSS: Maximun Segment Size, tamanho máximo do segmento de dados. Um pacote MSS que ultrapasse o MSS dos roteadores por onde o túnel está estabelecido deve ser fragmentado antes de enviá-lo. Em alguns caso o PMTUD está quebrado ou os roteadores não conseguem trocar informações de maneira eficiente e causam uma série de problemas com transferência HTTP, FTP, POP, etc... Neste caso Mikrotik proporciona ferramentas onde é possível interferir e configurar uma diminuição do MSS dos próximos pacotes através do túnel visando resolver o problema.



Redes Brasil

Mais sobre perfis



- Bridge: Bridge para associar ao perfil, isso mesmo, é possível associar um túnel PPTP L2TP a uma bridge e fazer um "LAN2LAN" entre dois ROUTERs utilizando a função BCP.

- Incoming/Outgoing Filter: Nome do canal do firewall para pacotes entrando/saindo.

Ou seja, é possível colocarmos uma política de firewall apenas para os usuários que estejam associados a aquele perfil.

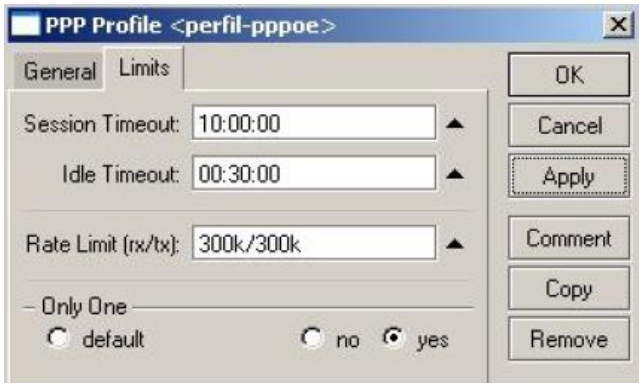
- Address List: Lista de endereços IP para associar ao perfil.

Ou seja, podemos ainda criar grupos a partir desdes clientes, e por exemplo, fazer uma política de rotas, uma política QoS diferenciado.

- DNS Server: Configuração dos servidores DNS a atribuir aos clientes. Se não configurado, o servidor passará aos clientes o seu próprio ip se configurado como cache de dns e mais os ips configurados em /ip dns

- Use Compression/Encryption/Change TCP MSS: caso estejam em default, vão associar ao valor que está configurado no perfil default-profile.

Mais sobre perfis



- Session Timeout: Duração máxima de uma sessão PPP (muito útil se utilizado em VPNs, porque, pode ser que o usuário se esqueça de desconectar da VPN quando finalizar o uso. Com isso consumindo recursos)

- Idle Timeout: Período de ociosidade na transmissão de uma sessão. Se não houver tráfego IP dentro do período configurado, a sessão é terminada.

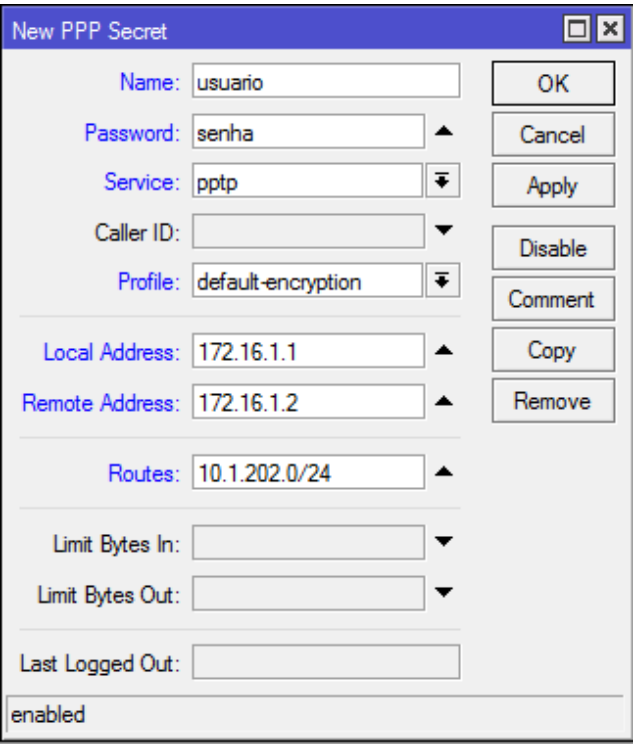
- Rate Limit: Limitação da velocidade na forma rx/tx.

Pode ser usado também na forma rx-rate/tx-rate rx-burst-rate/tx-burstrate rx-burst-threshould/tx-burst-threshould burst-time priority rx-rate-min/tx-rate-min.

- Only One: Permite apenas uma sessão para o mesmo usuário.

Redes Brasil

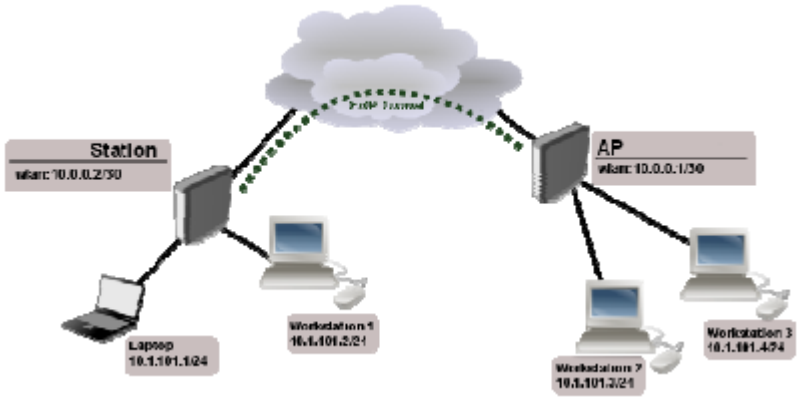
Mais sobre o a base de usuários



- Service: Especifica o serviço disponível para este cliente em particular.
- Caller ID: Se VPN, será um IP, se um pppoe, o MAC
- Local/Remote Address: Endereço IP Local (servidor) e remote(cliente) que poderão ser atribuídos a um cliente em particular.
- Limits Bytes IN/Out: Quantidade em bytes que o cliente pode trafegar por sessão PPPoE.
- Routes: Rotas que são criadas do lado do servidor para esse cliente especifico. Várias rotas podem ser adicionadas separadas por vírgula.

Redes Brasil

Túneis EoIP



- EoIP(Ethernet over IP) é um protocolo proprietário Mikrotik para encapsula mento de todo tipo de tráfego sobre o protocolo IP.

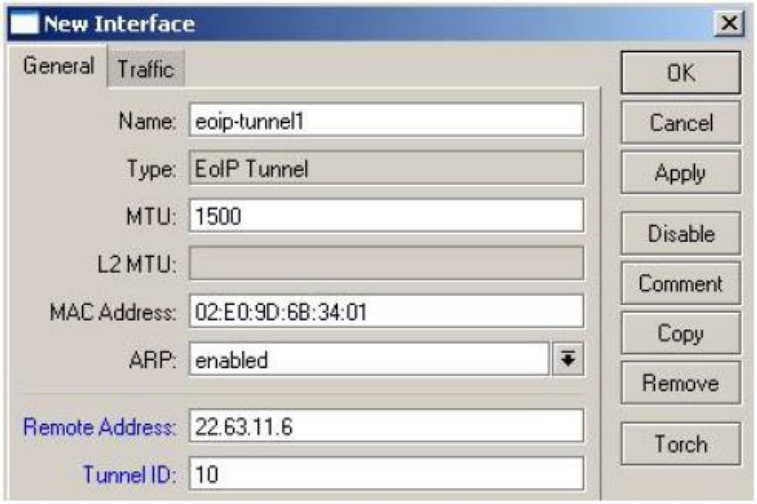
- Quando habilitada a função de Bridge dos roteadores que estão interligados através de um túnel EoIP, todo o tráfego é passado de uma lado para o outro de forma transparente mesmo roteado pela internet e por vários protocolos.

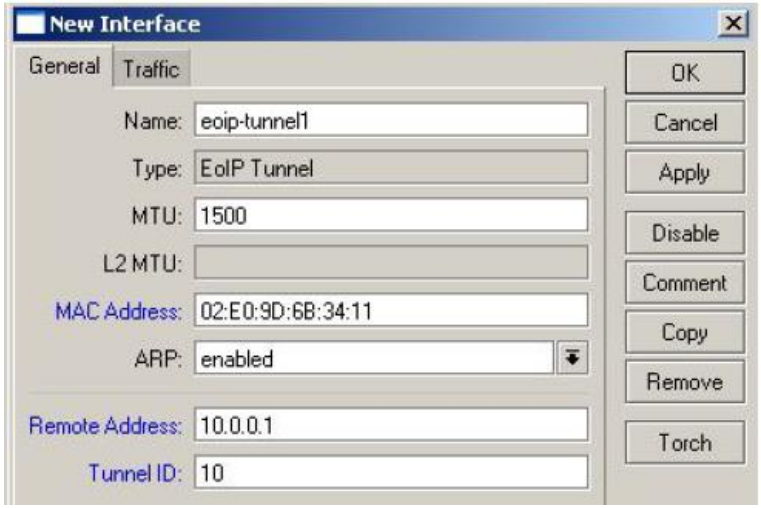
- O protocolo EoIP possibilita:
  - Interligação em bridge de LANs remotas através da internet.
  - Interligação em bridge de LANs através de túneis criptografados.

- A interface criada pelo túnel EoIP suporta todas funcionalidades de uma interface ethernet. Endereços IP e outros túneis podem ser configurados na interface EoIP. O protocolo EoIP encapsula frames ethernet através do protocolo GRE.

Túneis EoIP

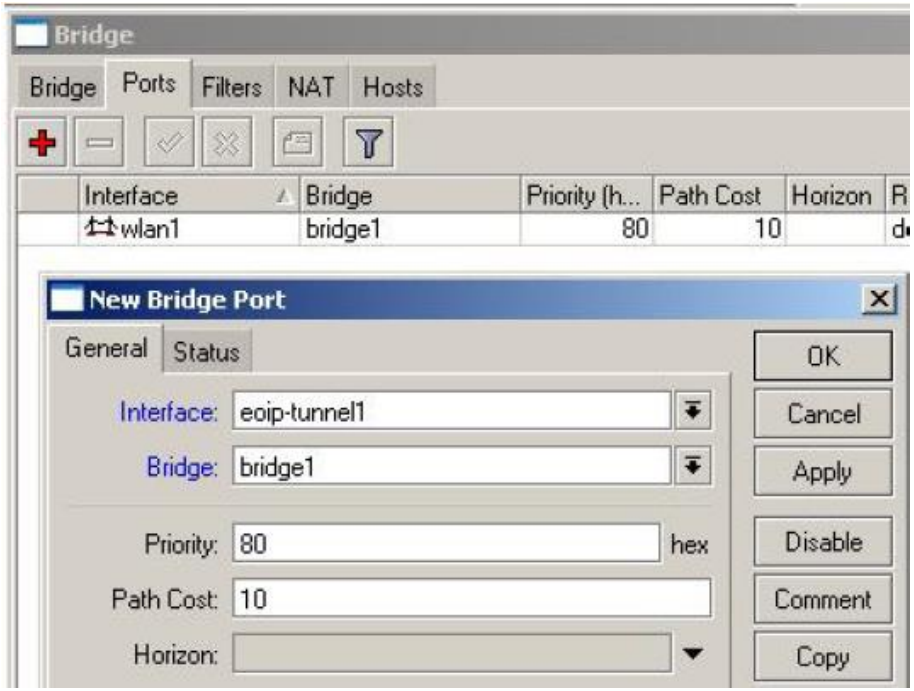
- Criando um túnel EoIP entre as redes por trás dos roteadores 10.0.0.1 e 22.63.11.6.
- O MTU deve ser deixado em 1500 para evitar fragmentação.
- O túnel ID deve ser igual para ambos.

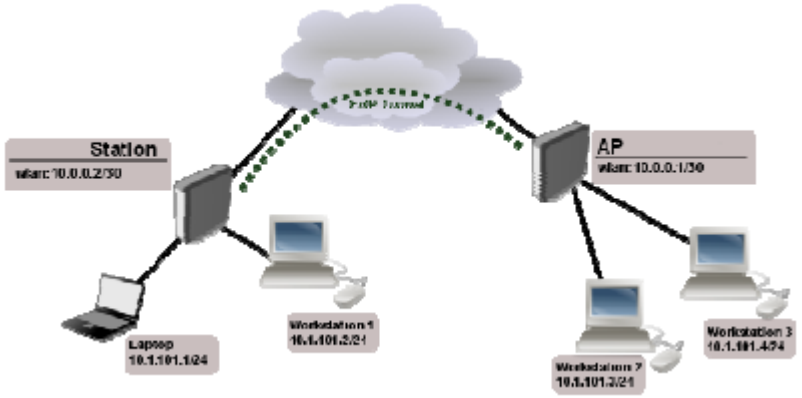




Redes Brasil

Túneis EoIP





- Adicione a interface EoIP a bridge, juntamente com a interface que fará parte do mesmo domínio de broadcast.

Redes Brasil

IPSEC

- Proporciona uma estrutura completa segura para vpns que atravessem a internet
- É normalmente utilizado para interligação de diversas empresas, órgãos públicos sistemas de cartões de crédito.
- Assegura a confidencialidade, quer dizer, somente as “pessoas” autorizadas podem ver os dados sensíveis. Adota métodos de encriptação e controle de acesso para isto.
- Também conta com um mecanismo de revisão de integridade dos dados que garante que não tenham sido modificados por alguém não autorizado.
- Internet Procotol Security é um conjunto de protocolos definido pela IETF para garantir a troca segura de pacotes IP/IPv6 através de redes não seguras (Internet).

IPSEC

- IPSec se pode dividir nos seguintes grupos:
- –Autentication Header (AH) - RFC 4302 para integridade e autenticação
- –Encapsulating Security Payload (ESP) - RFC 4303 para confidencialidade
- –Internet Key Exchange (IKE) – É utilizado para a criação e distribuição dinâmica de chaves de criptografia para AH e ESP.

Alguns conceitos sobre IPSEC

- Fase 1: Os pares devem concordar com os algoritmos utilizados em mensagens IKE e autenticar.

Nesta fase tem que combinar os seguintes itens:

- authentication method
- DH group (no Mikrotik não é por numero do numero)
- encryption algorithm
- exchange mode
- hash algorithm
- NAT-T
- DPD and lifetime (optional)

DH Group 1	768 bit MODP group
DH Group 2	1024 bits MODP group
DH Group 3	EC2N group on GP(2^155)
DH Group 4	EC2N group on GP(2^185)
DH Group 5	1536 bits MODP group

Alguns conceitos sobre IPSEC

- Fase 2: Os pares estabelecem uma ou mais SAs que serão usados pelo IPsec para criptografar dados. Todos os SAs estabelecidas pelo IKE daemon terão valores de vida (ou de limitação de tempo, após o qual SA se tornará inválida, ou quantidade de dados que podem ser criptografados por este SA, ou ambos).

Nesta fase tem que combinar os seguintes itens:

- Ipsec protocol
- mode (tunnel or transport)
- authentication method
- PFS (DH) group
- lifetime

Exemplo Configuração ipsec no Cisco Router

```
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
lifetime 54000
!
crypto isakmp key SENHAEXEMPLO address 0.0.0.0 0.0.0.0 no-xauth
crypto isakmp keepalive 120 5
!
crypto ipsec transform-set YES esp-3des esp-md5-hmac
!
crypto map ELETRO 3 ipsec-isakmp
 description EXEMPLO02
set peer host.dyndns.org dynamic
set security-association lifetime seconds 1800
set transform-set YES
 set pfs group2
match address EXEMPLO02
!
ip access-list extended EXEMPLO02
permit ip any 172.18.2.0 0.0.0.255
```

Redes Brasil

Exemplo de configuração IPSEC no RouterOS

```
/ip ipsec proposal
add auth-algorithms=md5 disabled=no enc-algorithms=3des lifetime=15h name=\
    vpn_eletrocisco pfs-group=modp1024
/ip ipsec peer
add address=200.1.1.1/32 auth-method=pre-shared-key comment=\
    "VPN_cisco new" dh-group=modp1024 disabled=no dpd-interval=disable-dpd \
    dpd-maximum-failures=5 enc-algorithm=3des exchange-mode=main \
    generate-policy=no hash-algorithm=md5 lifebytes=0 lifetime=30m \
    my-id-user-fqdn="" nat-traversal=no port=500 proposal-check=obey secret=\
    SENHAEXEMPLO send-initial-contact=yes
/ip ipsec policy
add action=encrypt disabled=no dst-address=0.0.0.0/0 dst-port=any \
    ipsec-protocols=esp level=use priority=0 proposal=vpn_eletrocisco \
    protocol=all sa-dst-address=200.1.1.1 sa-src-address=0.0.0.0 \
    src-address=172.18.2.0/24 src-port=any tunnel=yes
```

Redes Brasil

E aí subiu??

Como saber se a comunicação está ocorrendo?

Realizando um ping partindo das estações.

Porque não foram criadas rotas em minha tabela de roteamento, terei que fazê-las estaticamente?

Não o Ipsec encaminhará de acordo com as policies criadas.

Porque a tabela de SAs está vazia?

Só serão criadas SAs quando ocorrer a primeira tentativa de conexão.

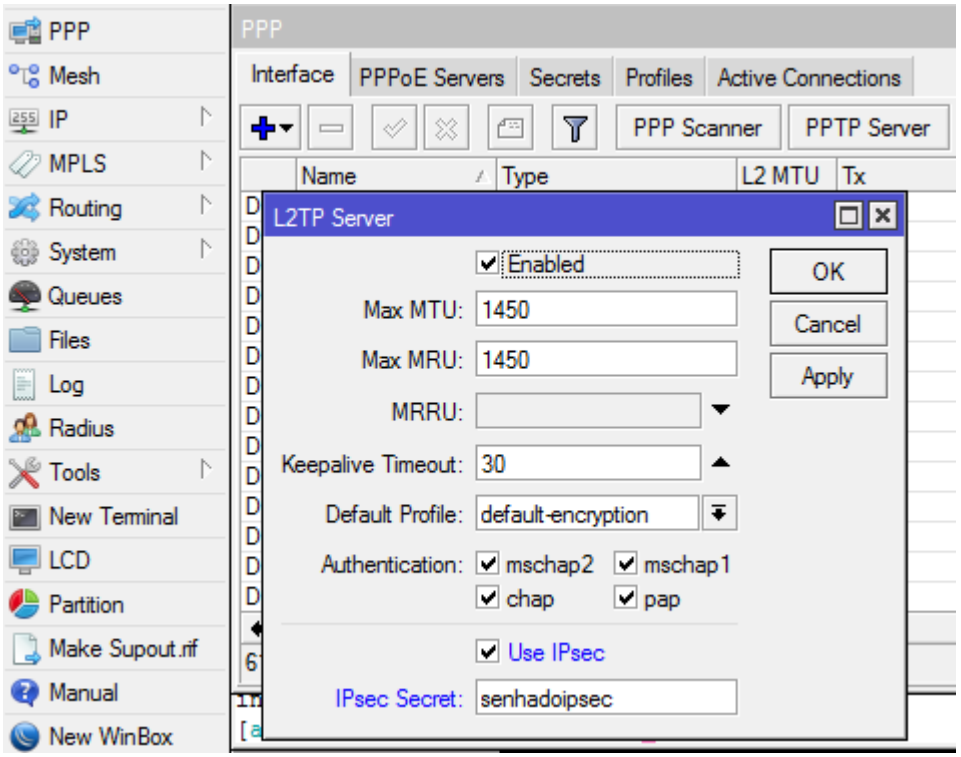
Como posso fazer o teste partindo da minha própria RB?

Utilizando um recurso chamado preferencial source, nele definindo um ip que faz parte da police por exemplo, se meu src-address for

172.18.2.0/24 e o dst-address: 10.123.123.1 eu posso criar

L2TP com IPSEC

O IPSec precisa de conectividade fim-a-fim verdadeira, ou seja é necessário que os dois equipamentos consiguam se enxergar, em resumo não funcionará em redes com nat, por padrão.



Uma forma de resolver esse "problema" é fechar um túnel l2tp que proverá conectividade fim-a-fim verdadeira, ou seja, Os ips que estabelecerão a comunicação serão ips locais

Redes Brasil

Redundancia de links (failover)

Uma das técnicas para checagem dos links é utilizar o netwatch.

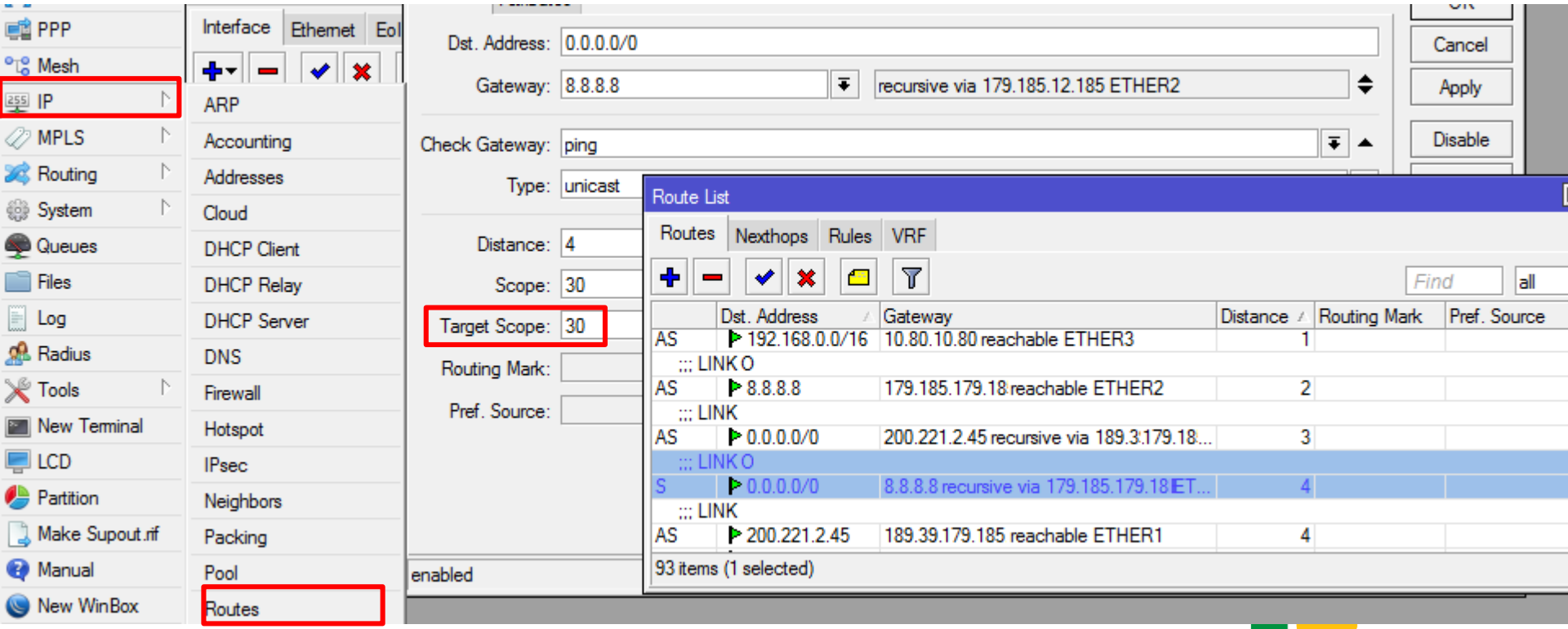
Porém como o netwatch é muito sensível, existem muitos falsos positivos.

Se colocarmos na tabela de rotas, o check gateway=ping ou arp, estaremos monitorando apenas a interface do próximo roteador, que geralmente está instalado nas dependências da empresa.

Uma das técnicas que utilizo é colocar um ip externo, geralmente o ultimo salto para sair da operadora.

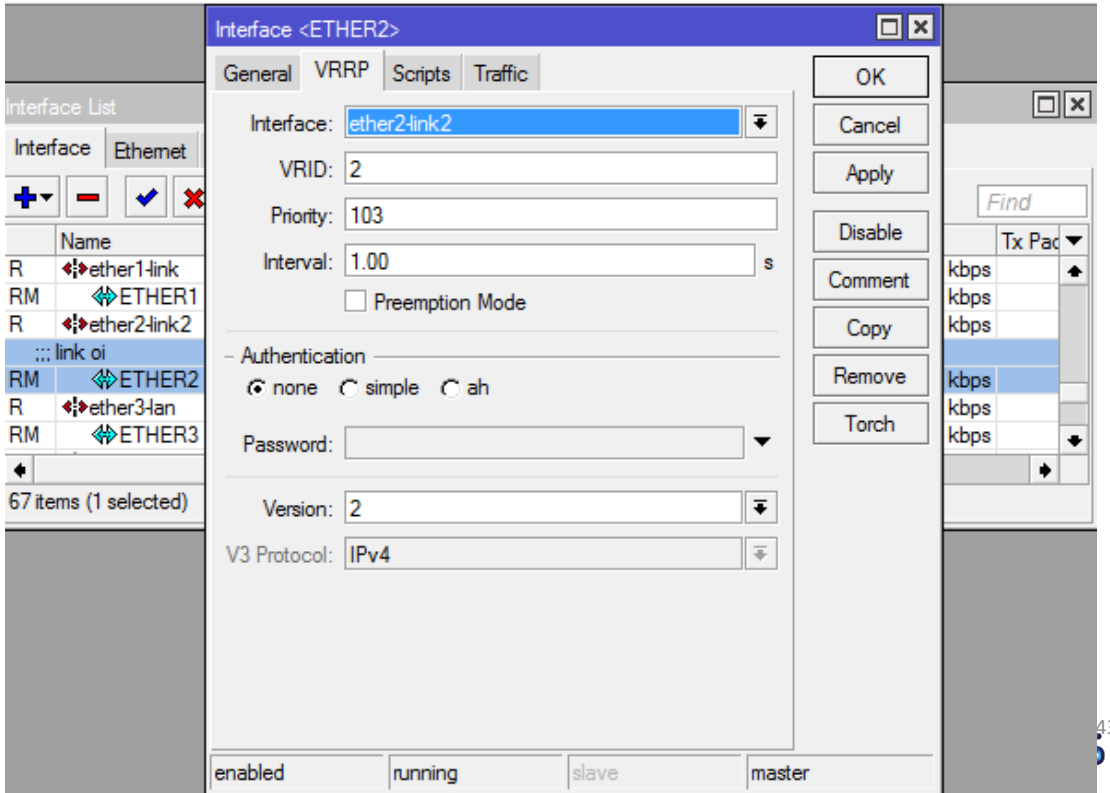
Redundancia de links (failover)

- Solução utilizando a tabela de rotas:



Equipamentos em HA (alta disponibilidade)

- O Mikrotik disponibiliza o recurso de VRRP, em que se um roteador para de responder as interfaces a ele atribuídas passam a não mais responder. Com isso o equipamento que estava em slave, automaticamente assume. Ainda é possível executar um script no caso da mudança de estado:
- Exemplo de uso:



OBRIGADO!

- Marcos A S Velez,

Mikrotik Training Partner,

MTCNA, MTCRE, MTCWE, MTCINE, MTCUME, MTCTCE

Mail: marcos@velez.com.br

Perguntas ?