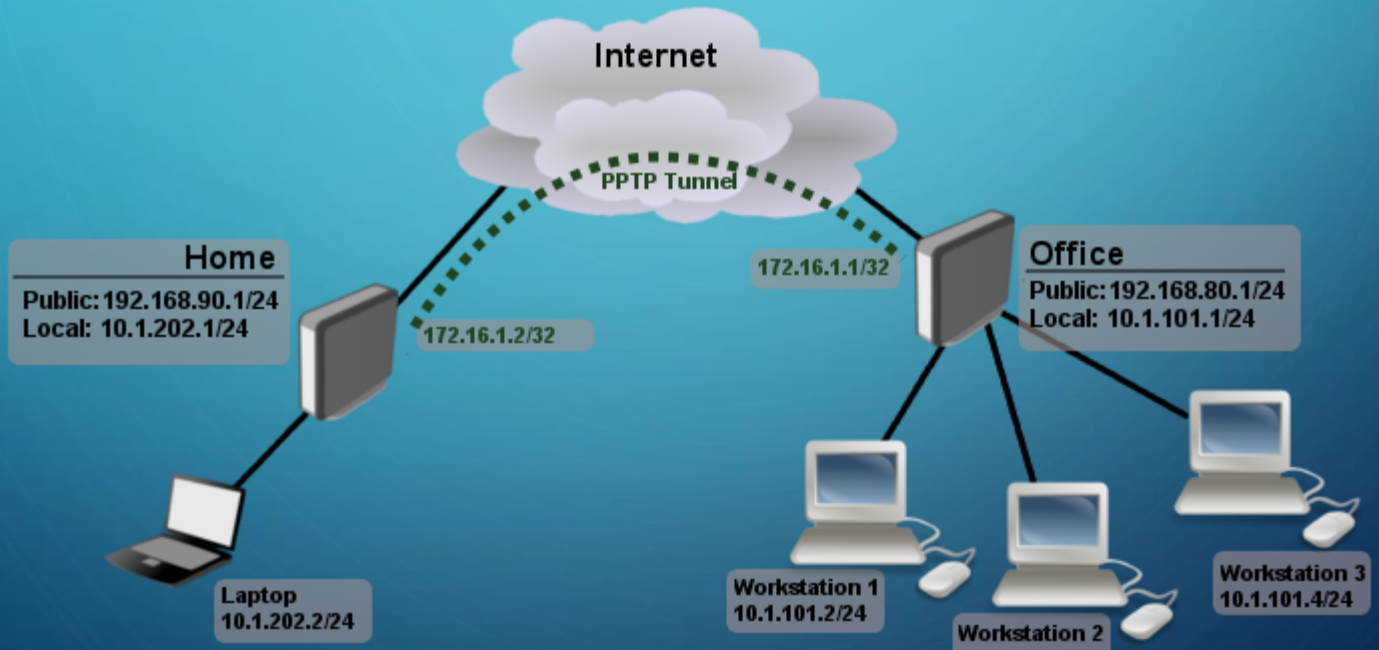
VPNS
BY RICK FREY

www.rickfreyconsulting.com

WHAT IS A VPN?

- A Virtual Private Network is a means by which two or more normally non-adjacent networks are connected through virtual “wires”.



MIKROTIK VPNS

- MikroTik routers can use 13 different tunneling protocols, all with there own strengths and weaknesses.
- This presentation will focus on which ones to use.

SUPPORTED TUNNEL PROTOCOLS

- Individual Tunnel Protocols
  - EOIP (Ethernet Over IP)
  - IPIP (IP over IP)
  - GRE (Generic Routing Encapsulation)
  - VLAN (Virtual LAN)
  - IPSEC (IP Security)
- PPP Based Tunnels
  - PPP (Point to Point Protocol)
  - PPPoE (Point to Point Protocol over Ethernet)
  - PPTP (Point to Point Tunneling Protocol)
  - L2TP (Layer 2 Transport Protocol)
  - SSTP (Secure Socket Tunneling Protocol)
  - OVPN (Open Virtual Private Network)
- MPLS Tunnels
  - VPLS
  - TE

CONSIDERATIONS FOR CHOOSING A TUNNEL

- Do both ends have static IPs?
- Will either side be traversing NAT?
- How secure does the information need to be?
- What type of traffic will be passed over the tunnel?
- How much bandwidth is needed for the tunnel?
- Will RADIUS be used?

STATIC VS DYNAMIC IPS

- If both ends of the tunnel have static IPs then all of the tunnels are an option.
- If static IP are not an option, Dynamic DNS can be used by these tunnels:
  - EOIP
  - GRE
  - PPTP
  - L2TP
  - SSTP
  - OVPN

WILL NAT BE A LIMITATION?

- When the tunnel needs to travers NAT, only 9 of the 13 protocols can be used. The follow tunnels are not able to be used through NAT:
  - VLANs
  - PPP
  - PPPoE
  - TE
  - VPLS

HOW SECURE DOES THE TUNNEL NEED TO BE?

Tunnel	Authentication Protocols	Encryption Protocols	Encryption Level
GRE	N/A	N/A	None
IPIP	N/A	N/A	None
VLAN	N/A	N/A	None
IPSEC	None	None	None, 64bits, 128bit,
	MD5	DES, 3DES, AES,	192bit, 256bit
	SHA1	Blowfish, Twofish,	
	SHA256	Camellia	
	SHA512		
PPPoE	PAP	None	None or
	CHAP	MPPE 40bit	40bit or 128bit
	MSCHAP v1	MPPE 128bit	
	MSCHAP v2		

HOW SECURE DOES THE TUNNEL NEED TO BE?

PPtP	PAP	None	None or
	CHAP	MPPE 40bit	40bit or 128bit
	MSCHAP v1	MPPE 128bit	
	MSCHAP v2		
L2TP	PAP	None	None or
	CHAP	MPPE 40bit	40bit or 128bit
	MSCHAP v1	MPPE 128bit	
	MSCHAP v2		
OVPN	None	None	None
	MD5	Blowfish 128	128bit, 192bit, or
	SHA1	AES 128	256bit
		AES 192	
		AES 256	

HOW SECURE DOES THE TUNNEL NEED TO BE?

EOIP	N/A	N/A	None
SSTP	PAP	None	None or
	CHAP	MPPE 40bit	40bit or 128bit
	MSCHAP v1	MPPE 128bit	or 256bit
	MSCHAP v2	TLS 1.0	
	TLS 1.0		
VPLS	N/A	N/A	None
TE	N/A	N/A	None

WHICH TUNNELS ARE THE MOST SECURE?

- In order of Highest to Lowest security (not including tunnels without encryption):
  - IPSEC (Hands down, the most secure)
  - OVPN
  - SSTP
  - PPTP & L2TP (Should not be used for important data)

WHAT TYPE OF TRAFFIC WILL BE PASSED?

- Will the traffic be Layer 2 or Layer 3? All of the tunnels will handle Layer3, but the following will also handle Layer 2 transport:
  - EOIP
  - PPTP
  - L2TP
  - SSTP
  - OVPN (has an additional UDP limitation)
  - PPPoE
  - TE
  - VPLS
- All of these tunnels have MTU considerations to be taken into account.

IS USING RADIUS A FACTOR

- Only the following tunnels can be used with RADIUS:
  - PPP
  - PPTP
  - L2TP
  - SSTP
  - OVPN
  - PPPoE

HOW MUCH BANDWIDTH IS NEEDED?

- This may be the single biggest concern. Only 4 tunnel types loose less than 10% of the available bandwidth:
  - TE & VPLS tunnels keep about 95% of the available bandwidth
  - IPSEC can keep 96.5% as long as both routers have an encryption co-processor
  - VLANs maintain about 84% of there available bandwidth.

- All of tunnel types lose at least 70% of the bandwidth.

HOW TO GET MORE BW

- Increase the MTU… If this is a possibility then PPTP goes from 91.2% loss to only 88.4% loss.
- Update your routers to take advantage of Fast Path and increased MTU sizes:
  - EOIP, IPIP, and GRE skyrocket from 72.5% loss to about 2.8% loss
- Lower the encryption level as well:
  - PPtP with an MTU of 1500 on ROS 6.34.3 using CHAP only has 5.2% loss as opposed to 91.2% under normal circumstances

OVERALL SUMMARY

- ROS improvement in just a few versions has made a huge impact on VPN performance.
- Fast Path works well for tunnels and is worth upgrading for.
- If you can take advantage of increased MTU sizes… do it!

QUESTIONS?