MikroTik IPSEC Configuration Worksheet

Purpose
The purpose of this worksheet is to gather all the information about the tunnel prior to implementation or changes. Be as specific as possible when filling this worksheet out.

Organization A Contact Information	
Name	
Phone #	
email	
Street Address	
City State	
Zip Code	

Organization B Contact Information	
Name	
Phone #	
email	
Street Address	
City State	
Zip Code	

Network Information		
Property	**Client A**	**Client B**
Hardware Platform		
OS Version		
IKE Phase 1		
Peer Address		
Port (integer:0..65535; Default = 500)		
Local Address (Local ISAKMP SA address on the router used by the peer) Not normally set		
Authentication method: (default = pre-shared-key) -pre-shared-key - authenticate by a password (secret) string shared between the peers -rsa-signature - authenticate using a pair of RSA certificates -rsa-key - authenticate using a RSA key imported in IPsec key menu. -pre-shared-key-xauth - mutual PSK authentication + xauth username/password. passive parameter identifies server/client side -rsa-signature-hybrid - responder certificate authentication with initiator Xauth. passive parameter identifies server/client side		
Passive (Yes | No Default = No)		
Secret (Preshared Key)		
Exchange Mode (aggressive | base | main | main-l2tp; Default: main)		
Send Initial Contact (yes | no; Default: yes)		
NAT Traversal (yes | no; Default: no) (ESP Only)		
Proposal Check (claim | exact | obey | strict; Default: obey)		
Hash Algorithm (md5 | sha1 | sha256 | sha512; Default: sha1)		
Encryption Algorithm (3des | aes-128 | aes-192 | aes-256 | blowfish camellia-128 | camellia-192 | camellia-256 | des; Default: aes-128)		
Mode Configuration (none | request-only | string; Default: none)		
DH Group (ec2n155 | ec2n185 | modp1024 | modp1536 | modp2048 | modp3072		
Generate Policy (no | port-override | port-strict; Default: no)		
Lifetime		
Lifebytes		
Dead Peer Detection Interval		
DPD Maximum Failures (integer: 1..100; Default: 5)		

IKE Phase 2		
IPSEC Protocols (ah | esp |ah&esp; Default: esp)		
Auth Algorithm (md5|sha1|null|sha256|sha512; Default: sha1)		
Encryption Algorithm (null|des|3des|aes-128-cbc|aes-128-cbc aes-128gcm | aes-192-cbc | aes-192-ctr|aes-192-gcm|aes-256-cbc |aes-256-ctr|aes-256-gcm | blowfish|camellia-128 camellia-192|camellia-256|twofish; Default: aes-128-cbc)		
Lifetime		
PFS Group (ec2n155 | ec2n185 | modp1024 | modp1536 | modp2048 | modp3072		

Security Policies		
Source Address		
Source Port		
Destination Address		
Destination Port		
Protocol (all | egp | ggp| icmp | igmp | ip-encap | tcp | udp | ipsec Default: all)		
SA Source Address		
SA Destination Address		
Tunnel Mode or Transport Mode (Tunnel Mode usually requires NAT; Transport mode often requires routing)		