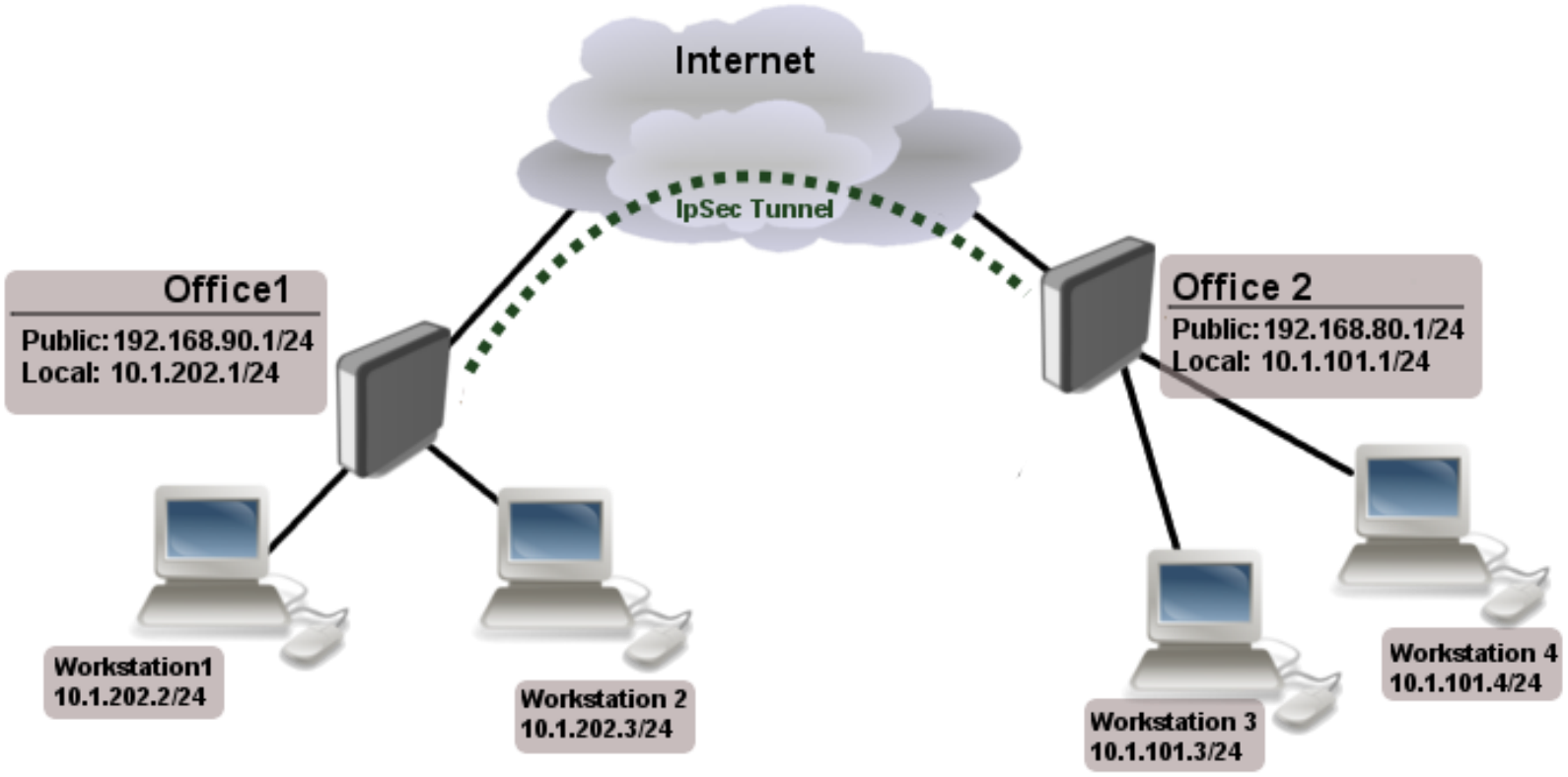
Rick Frey Consulting
www.rickfreyconsulting.com

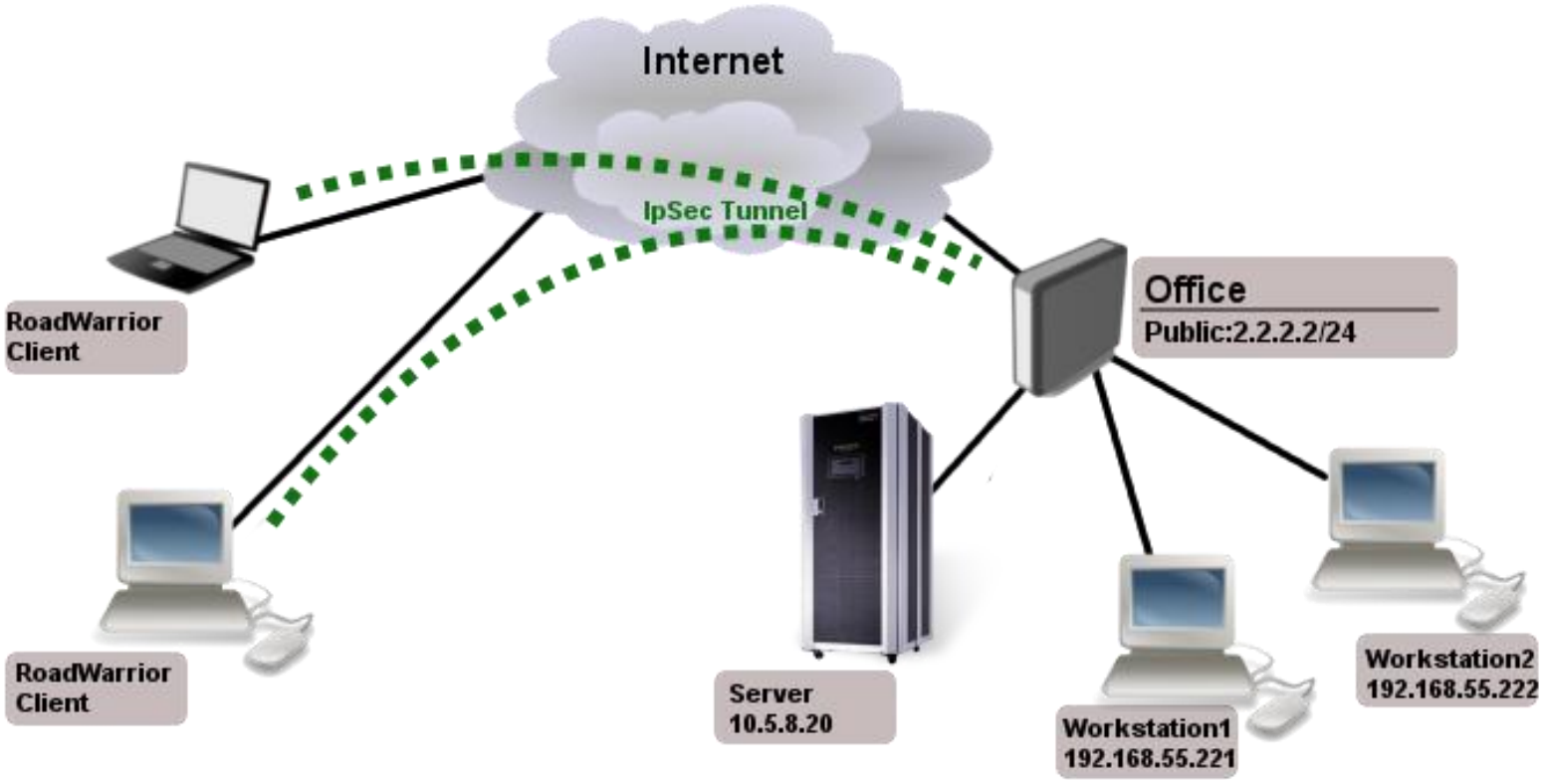
IPSEC

IPSEC

IPSEC used for Site to Site Tunnel



IPSEC used for Client to Gateway Tunnel



IPSEC

- Standardized in Nov 1998 by the IETF in a long list of RFCs
- The IPSEC standards include more possibilities than any one device can incorporate.
- Introduced during the 80386 CPU era
- Is considered to be the most secure tunneling method
- Usually has the least impact on performance of any tunnel (as long as the devices have an encryption co-processor)
  - RB-1000
  - RB-1100 Series
  - All CCRs & CRS Products
- Often used with other tunnels such as L2TP and IPIP

IPSEC – 5 Major Phases

- 1 - Define interesting traffic
- 2 - IKE phase 1 – key exchange phase
- 3 - IKE phase 2 – IPSEC policy and transform sets are processed
- 4 - Transfer data – After the tunnels are established you transfer the data.
- 5 - Tear down the tunnel

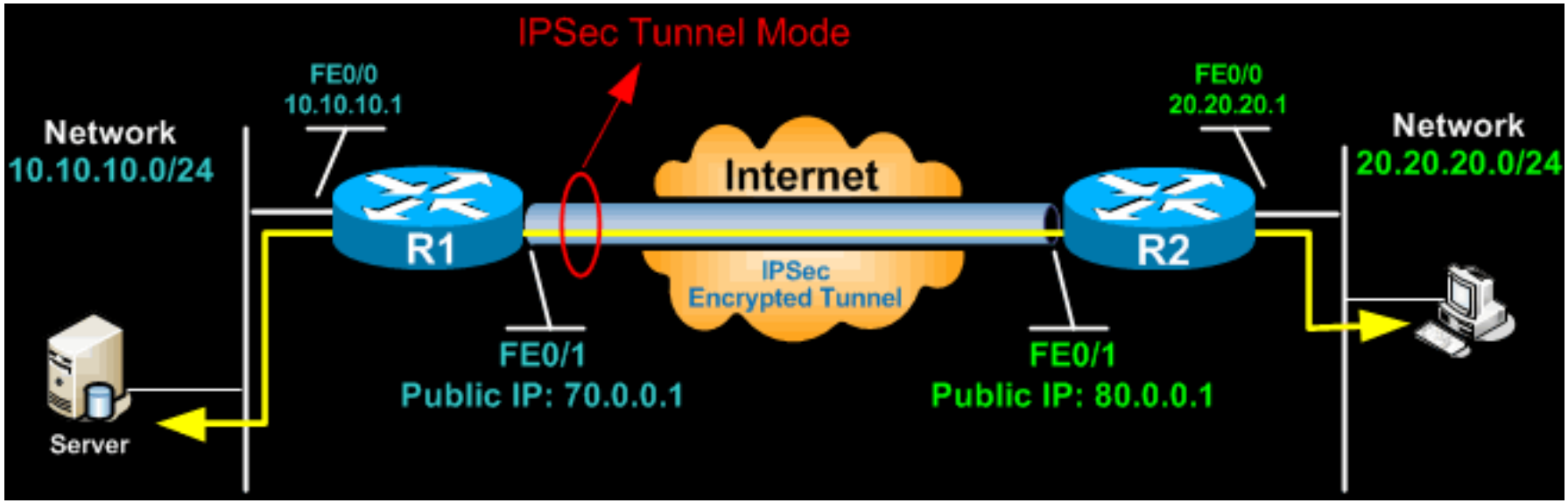
Step 1 – Define Interesting Traffic

- Specific polices must be set to define what traffic will pass through the tunnel. These policies must match on both sides of the tunnel.

- This is also the step where you define whether you will be using "Tunnel Mode" or Transport Mode."

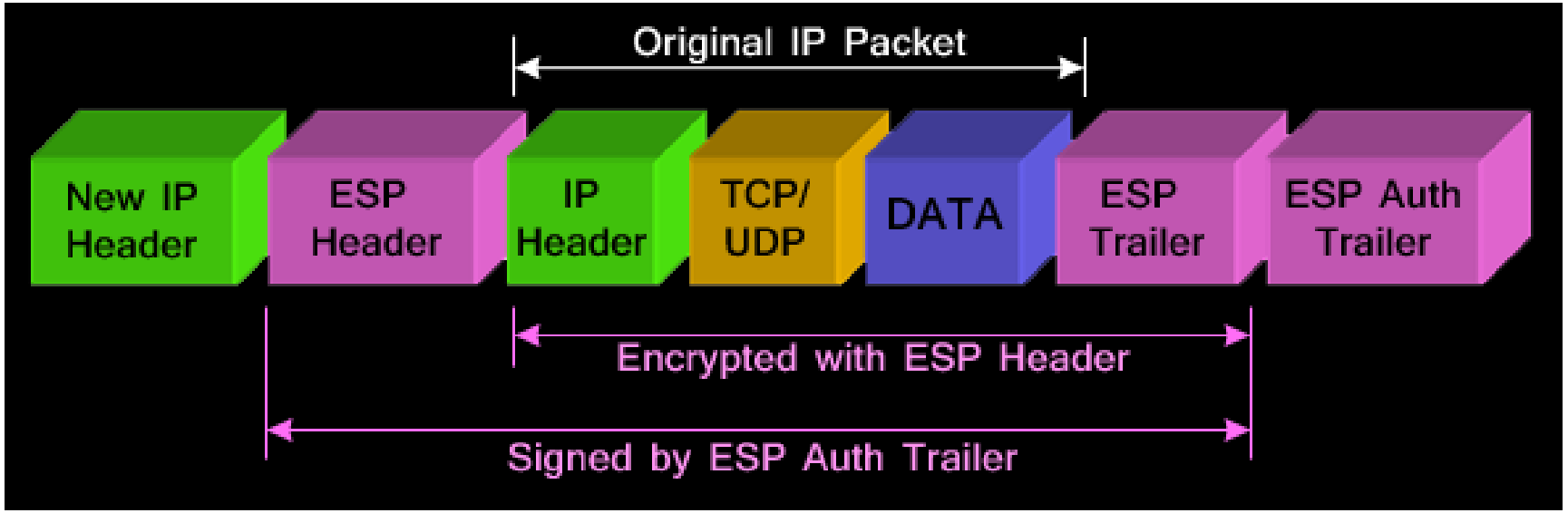
Tunnel Mode

- Most commonly used for Site to Site VPNs.
- Encapsulates the original IP packet with a new header, the entire original packet is encrypted.
- Will require some level of routing



Tunnel Mode

- Original IP packet in encapsulated with a new IP and ESP header & trailer

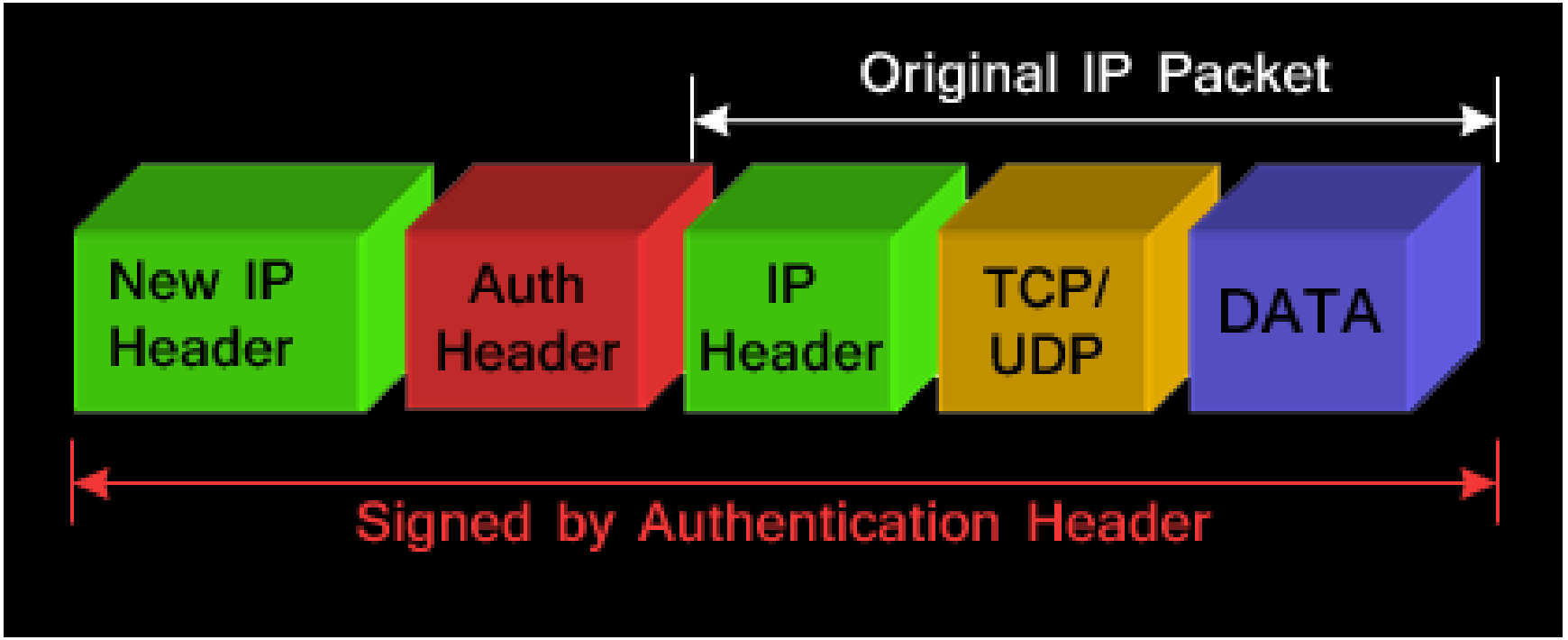


Tunnel Mode with AH Header

- The AH can be applied alone or together with the ESP, when IPSec is in tunnel mode.
- AH's job is to protect the entire packet. The AH does not protect all of the fields in the New IP Header because some change in transit, and the sender cannot predict how they might change. The AH protects everything that does not change in transit.
- AH is identified in the **New IP header** with an IP **protocol ID** of **51.**

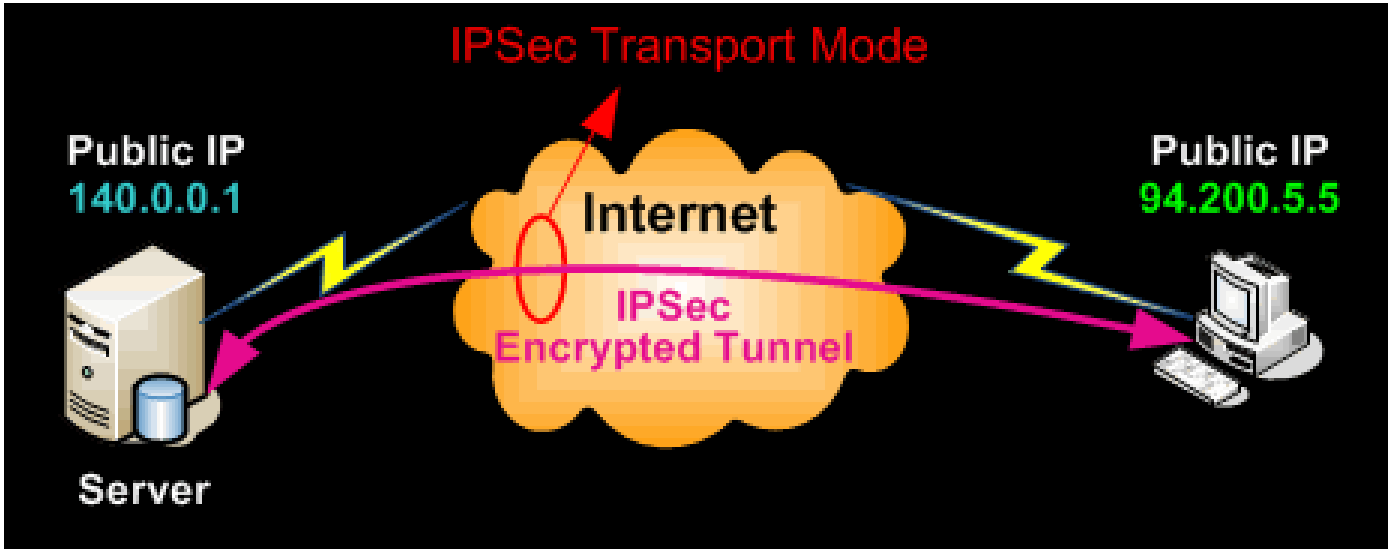
Tunnel Mode with AH Header

- The AH header can be used with or without ESP



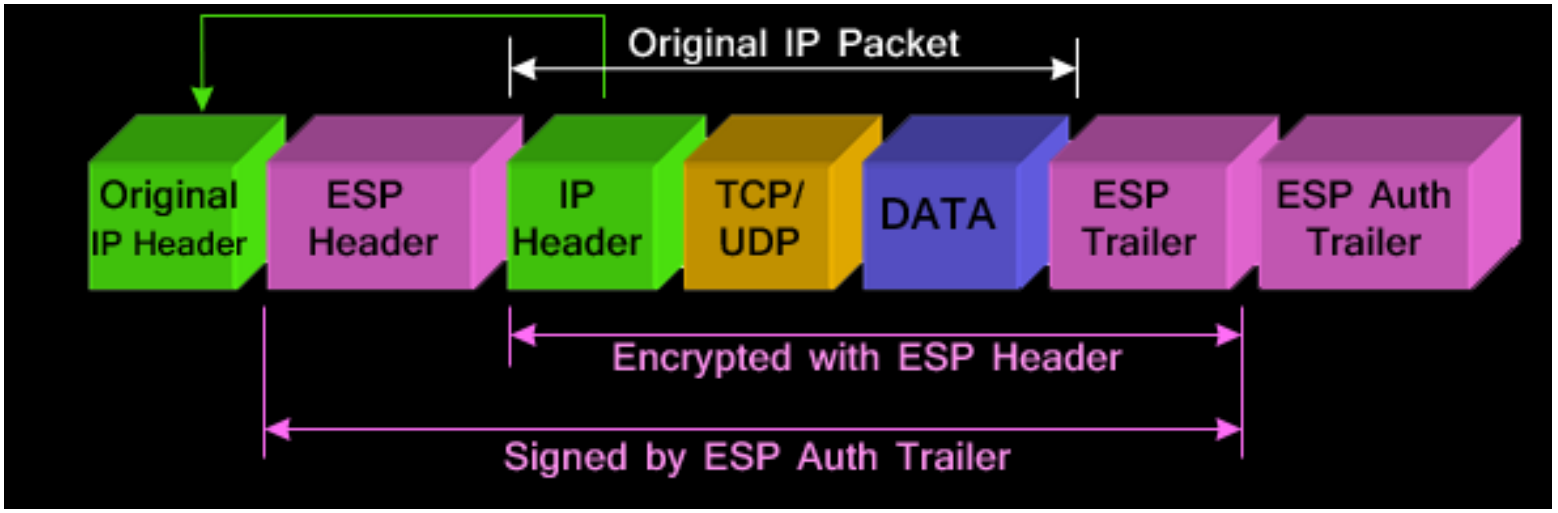
Transport Mode

- Most commonly used to connect a host to a remote network
- Often used with another tunnel protocol such as L2TP, IPIP, or GRE

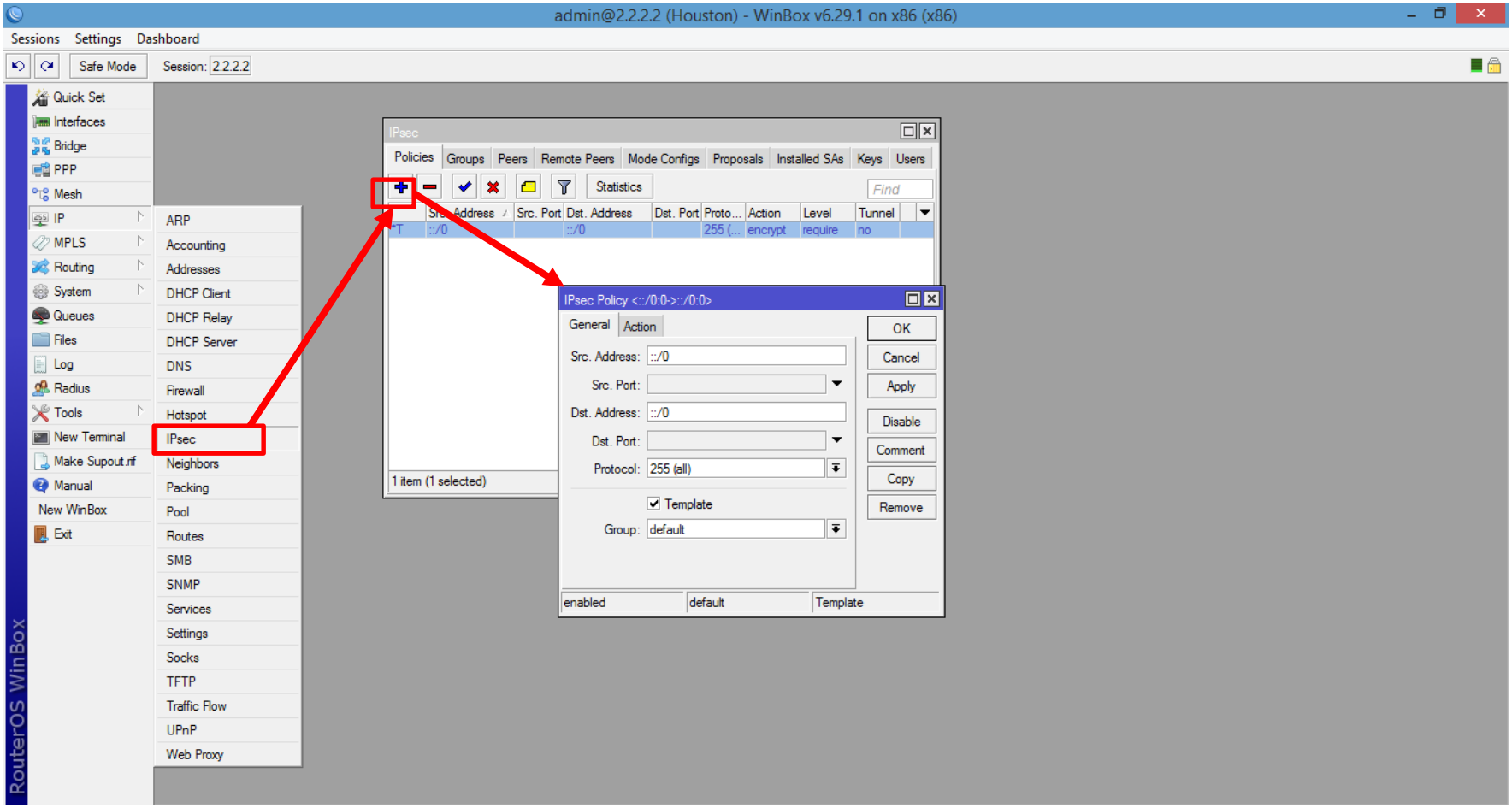


Tunnel Mode

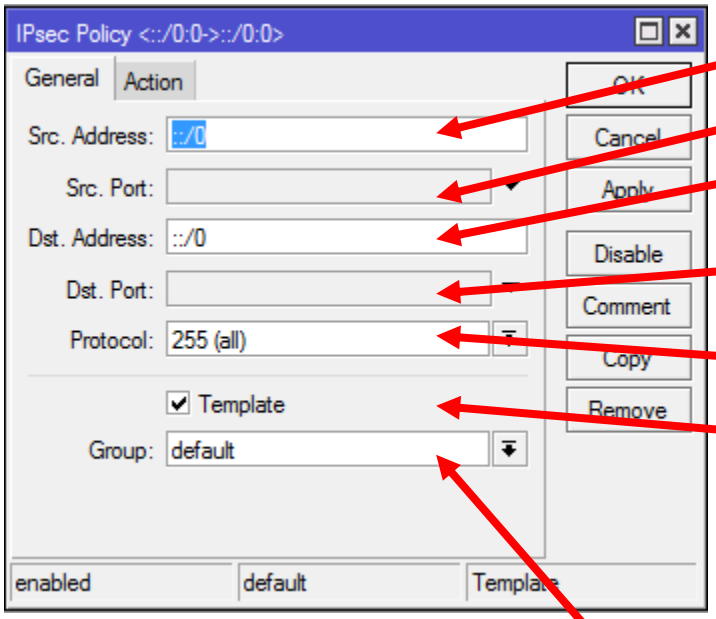
- The payload is encapsulated by the IPSEC headers and trailers. The original IP headers remain intact, except that the IP protocol field is changed to ESP (50) or AH (51), and the original protocol value is saved in the IPsec trailer to be restored when the packet is decrypted.
- AH mode can also be used (not shown in this image)



IPSEC Polices (Defining Traffic)

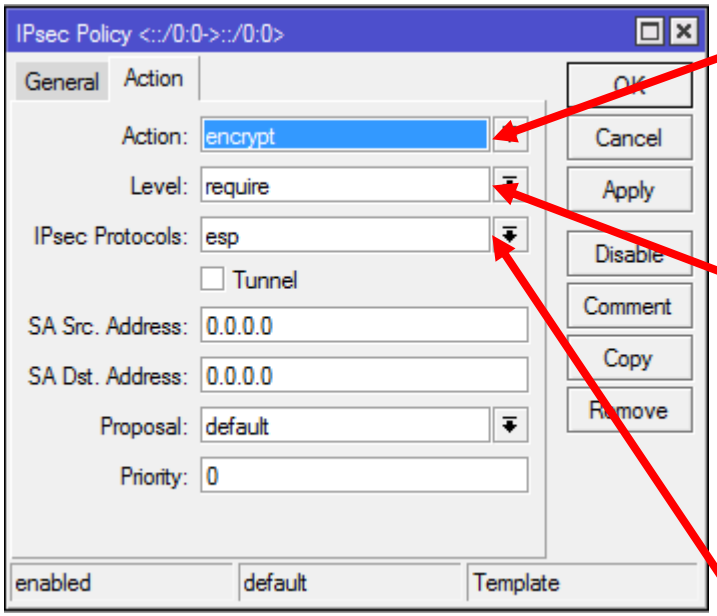


IPSEC Polices (Defining Traffic)



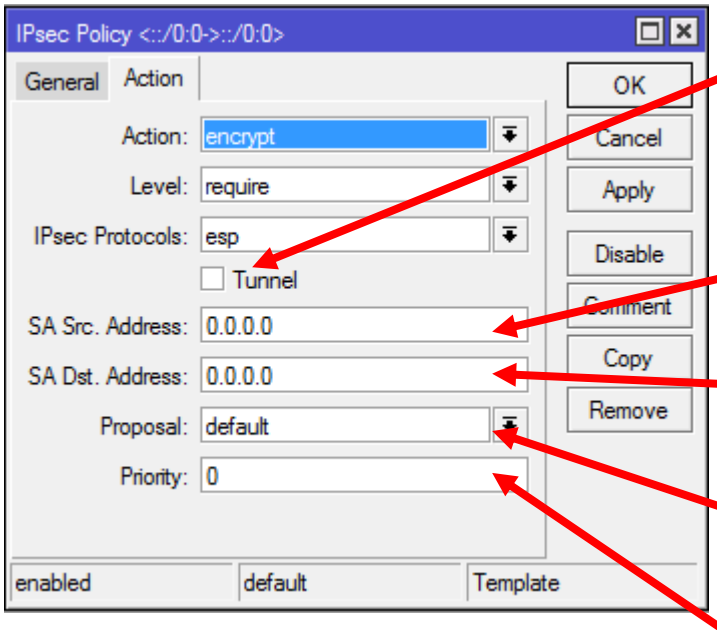
- Source IP prefix
- Source Port of the packet
- Destination address to be matched in packets
- Destination port to be matched in packets.
- IP packet protocol to match
- Creates a template and assigns it to specified policy group. Following parameters are used by template: src-address, dst-address - Requested subnet must match in both directions (for example 0.0.0.0/0 to allow all) protocol - protocol to match, if set to all, then any protocol is accepted proposal - SA parameters used for this template.
- Name of the policy group to which this template is assigned.

IPSEC Polices (Defining Traffic)



- Specifies what to do with packet matched by the policy
  - none - pass the packet unchanged
  - discard - drop the packet
  - encrypt - apply transformations specified in this policy and it's SA
- Specifies what to do if some of the SAs for this policy cannot be found
  - use - skip this transform, do not drop packet and do not acquire SA from IKE daemon
  - require - drop packet and acquire SA
  - unique - drop packet and acquire a unique SA that is only used with this particular policy
- Specifies which combo of AH and/ or ESP to use

IPSEC Polices (Defining Traffic)

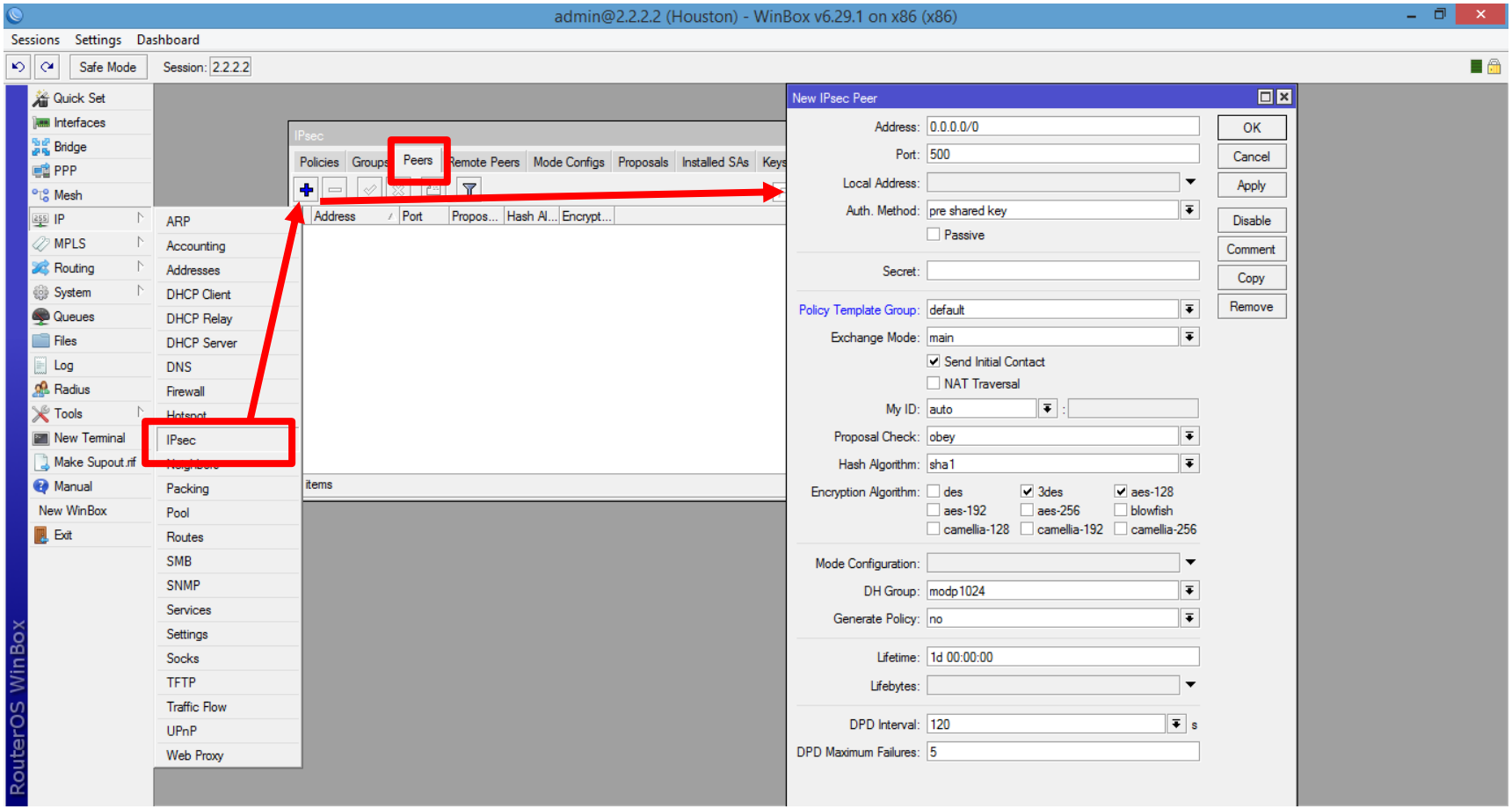


- Tunnel mode when checked, Transport mode when unchecked
- SA source IP/IPv6 address (local peer).
- SA destination IP/IPv6 address (remote peer).
- Name of the proposal template
- Policy ordering classificator (signed integer). Larger number means higher priority.

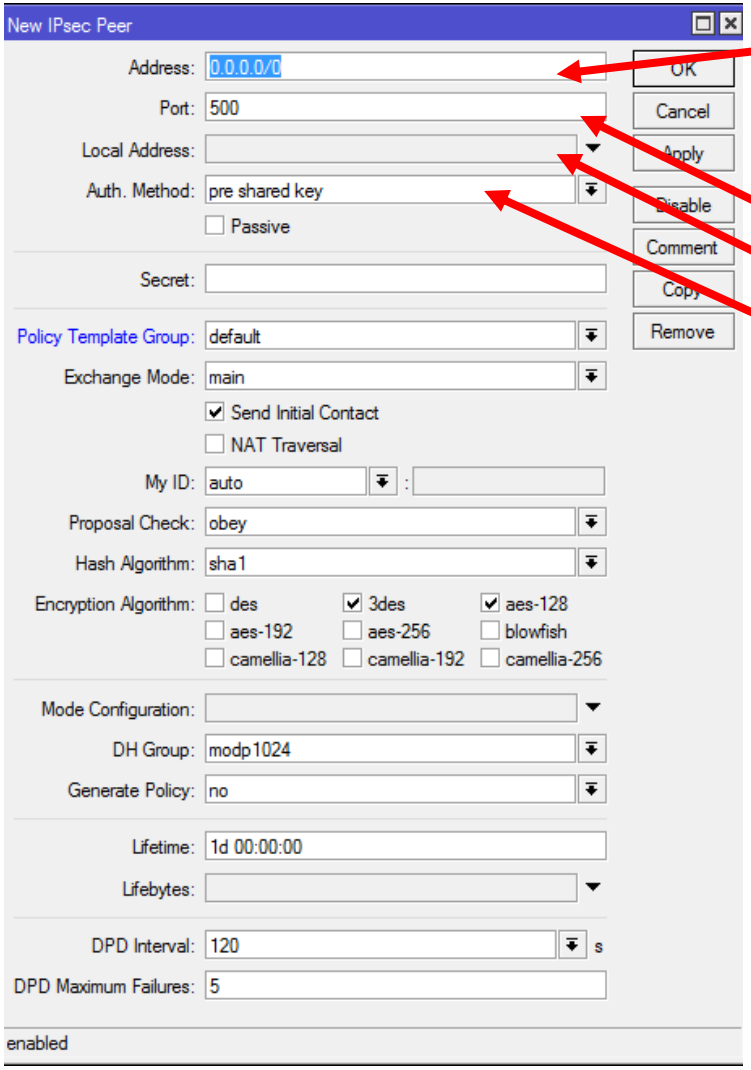
IKE Phase 1 – Key Exchange Phase

- **Phase 1 -** The peers agree upon algorithms they will use in the following IKE messages and authenticate. The keying material used to derive keys for all SAs and to protect following ISAKMP exchanges between hosts is generated also. This phase should match following settings:
  - authentication method
  - DH group
  - encryption algorithm
  - exchange mode
  - hash alorithm
  - NAT-T
  - DPD and lifetime (optional)

IKE phase 1 – Key Exchange Phase

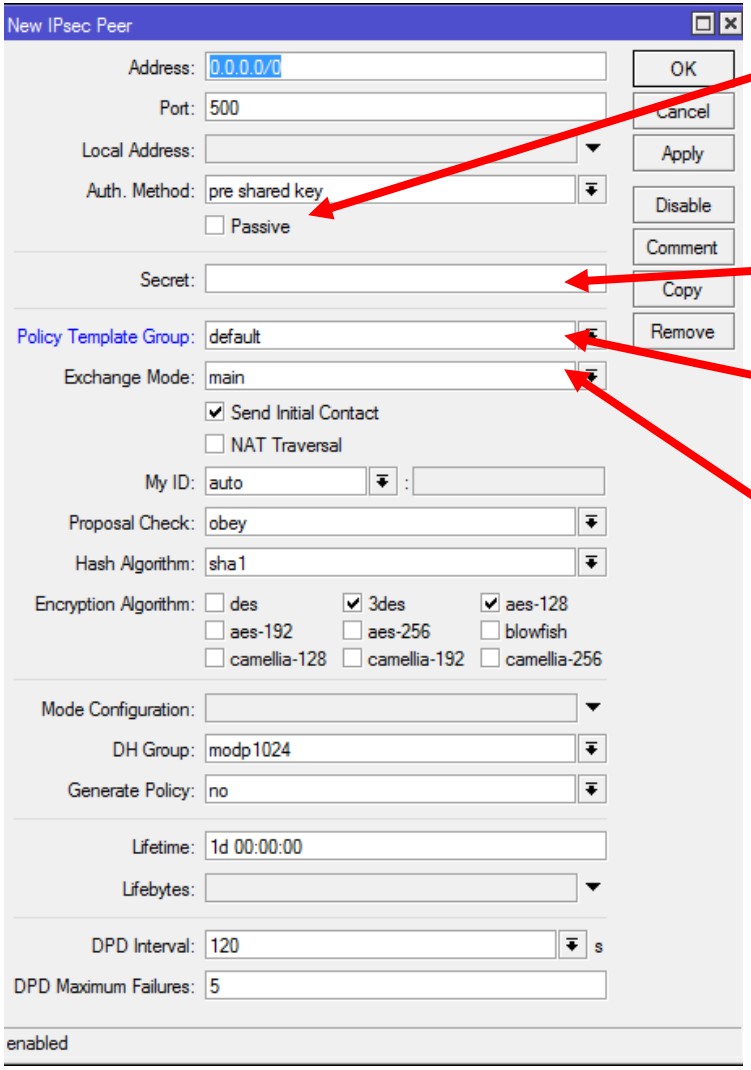


Creating a New IPSEC Peer



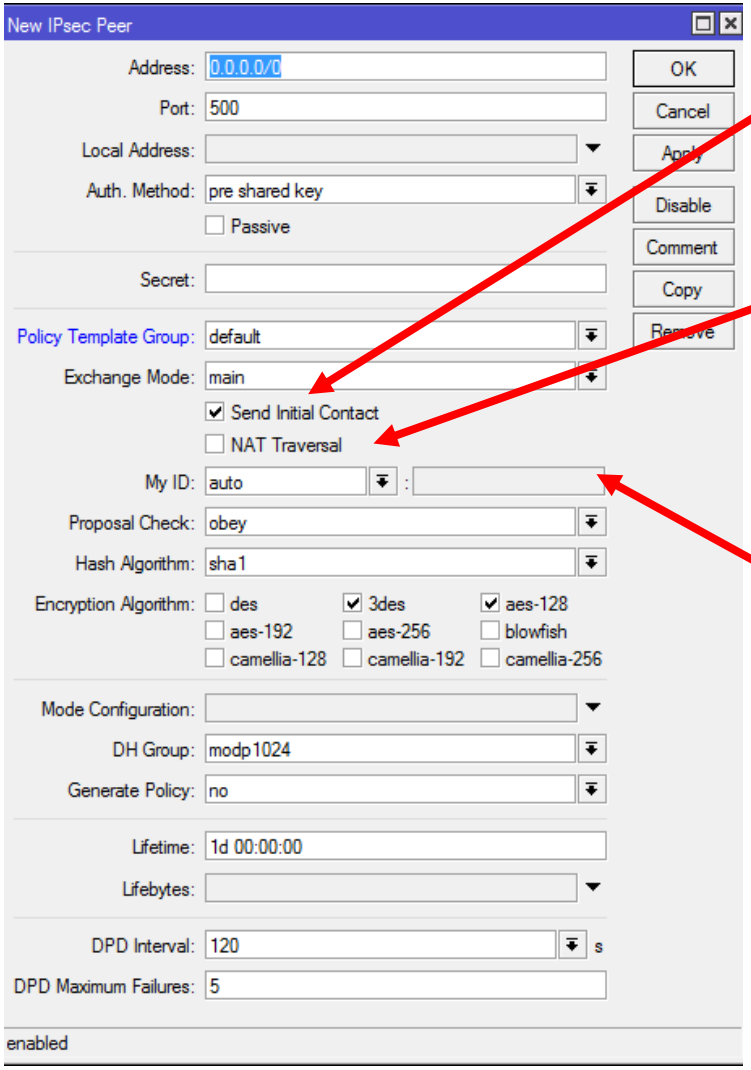
- If remote peer's address matches this prefix, then the peer configuration is used in authentication and establishment of **Phase 1**. If several peer's addresses match several configuration entries, the most specific one (i.e. the one with largest netmask) will be used.
- Port used for IPSEC traffic.
- Local Address (Normally not used)
- Authentication method:
  - 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

Creating a New IPSEC Peer



- When passive mode is enabled will wait for remote peer to initiate IKE connection. Enabled passive mode also indicates that peer is xauth responder, and disabled passive mode - xauth initiator.
- Secret string (in case pre-shared key authentication is used). If it starts with '0x', it is parsed as a hexadecimal value.
- If generate-policy is enabled, responder checks against templates from the same group. If none of the templates match, Phase2 SA will not be established.
- Different ISAKMP phase 1 exchange modes according to RFC 2408. Do not use other modes then main unless you know what you are doing. **main-l2tp** mode relaxes rfc2409 section 5.4, to allow pre-shared-key authentication in main mode.

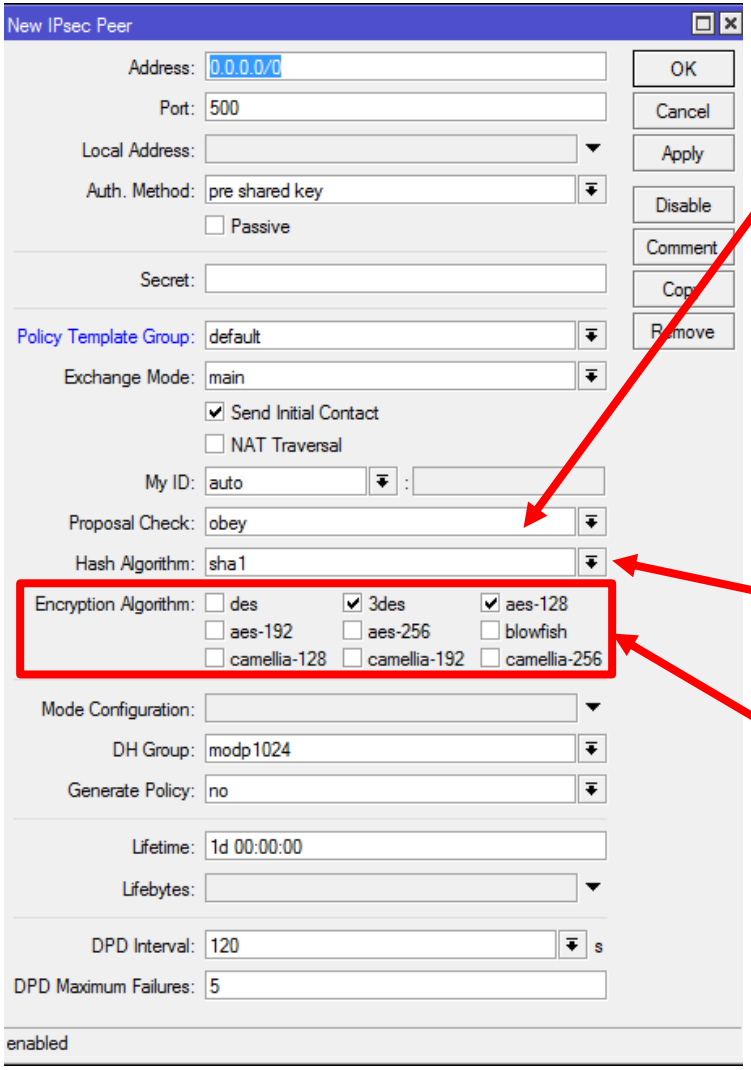
Creating a New IPSEC Peer



- Specifies whether to send "initial contact" IKE packet or wait for remote side, this packet should trigger removal of old peer SAs for current source address. Usually in road warrior setups clients are initiators and this parameter should be set to no.
- Use Linux NAT-T mechanism to solve IPsec incompatibility with NAT routers inbetween IPsec peers. This can only be used with ESP protocol (AH is not supported by design, as it signs the complete packet, including IP header, which is changed by NAT, rendering AH signature invalid). The method encapsulates IPsec ESP traffic into UDP streams in order to overcome some minor issues that made ESP incompatible with NAT.
- This parameter sets IKE ID to specified mode. It is possible to manually set two modes: FQDN and USER_FQDN.
  - **FQDN** - fully qualified domain name
  - **USER_FQDN** - specifies a fully-qualified username string, for example, "user@domain.com";
  - **auto** IP address is used as ID.

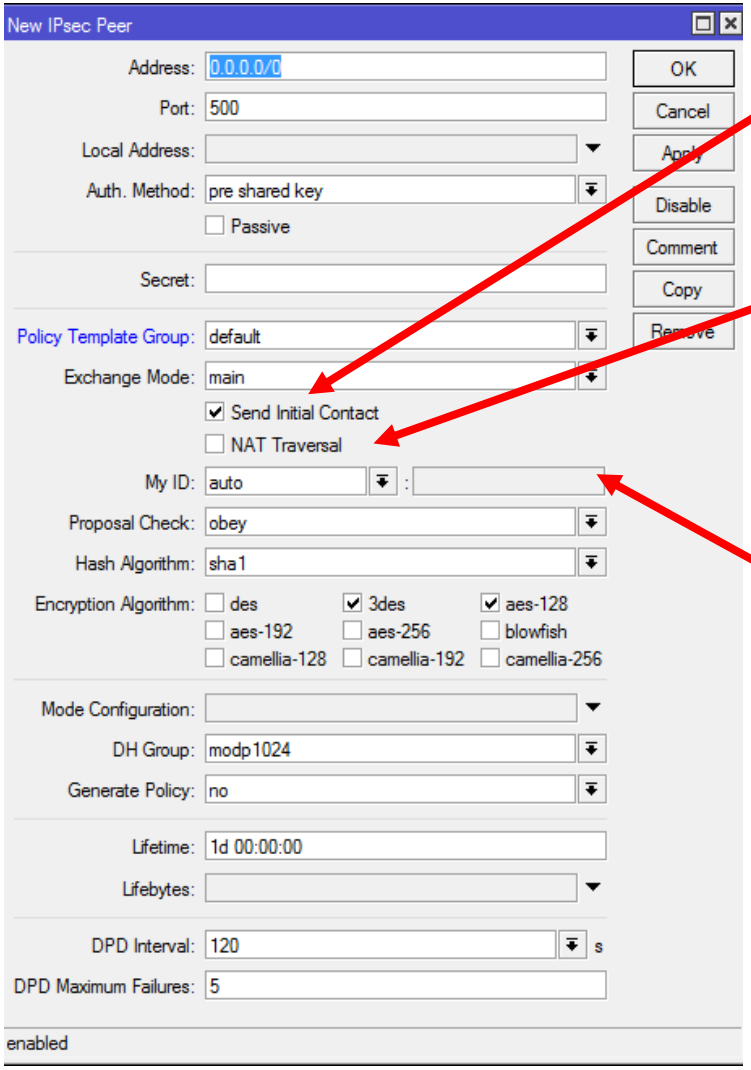
•responder will assign ip address if address-pool is specified, will send also DNS server addresses and split-include subnets (if defined).

Creating a New IPSEC Peer



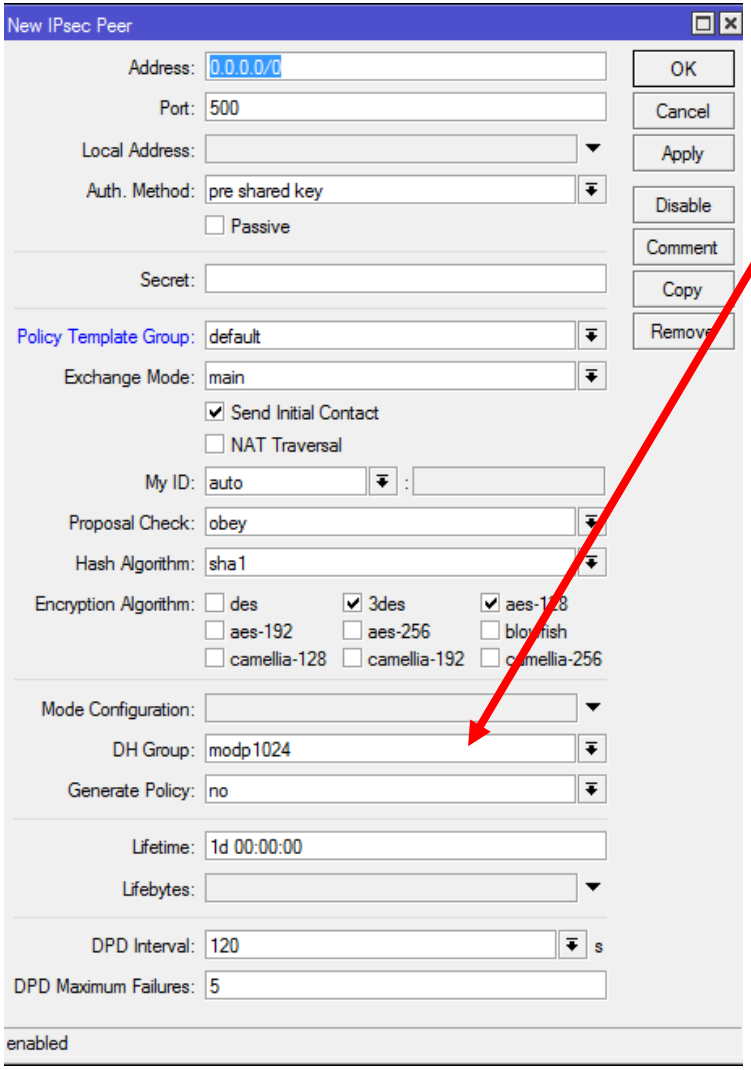
- Phase 2 lifetime check logic:
  - claim - take shortest of proposed and configured lifetimes and notify initiator about it
  - exact - require lifetimes to be the same
  - obey - accept whatever is sent by an initiator
  - strict - if proposed lifetime is longer than the default then reject proposal otherwise accept proposed lifetime
- Hashing algorithm. SHA (Secure Hash Algorithm) is stronger, but slower. MD5 uses 128-bit key, sha1-160bit key.
- Encryption algorithms that will be used by the peer.

Creating a New IPSEC Peer



- Name of the mode config parameters from mode-config menu. When parameter is set mode-config is enabled.
  - initiator peer on phase1 will send mode-config request and will set assigned IP address and DNS.
  - responder will assign ip address if address-pool is specified, will send also DNS server addresses and split-include subnets (if defined).

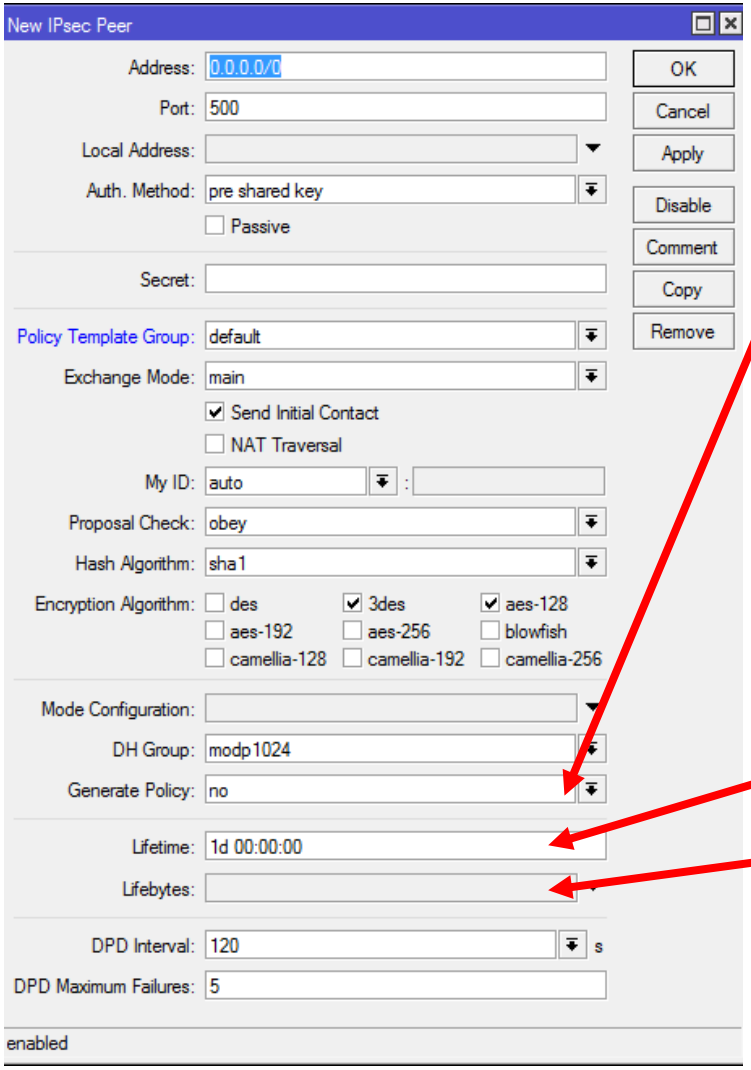
Creating a New IPSEC Peer



- Diffie-Hellman (DH) key exchange protocol allows two parties without any initial shared secret to create one securely. The following Modular Exponential (MODP) and Elliptic Curve (EC2N) Diffie-Hellman (also known as "Oakley") Groups are supported:

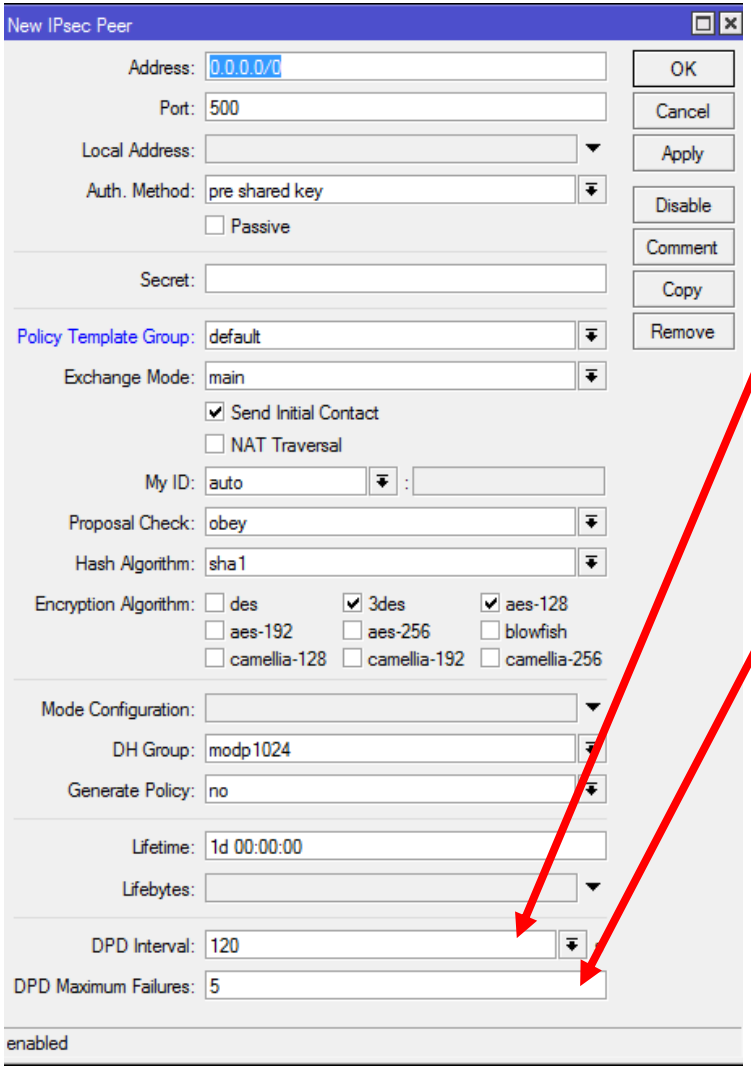
Diffie-Hellman Group	Name	Reference
Group 1	768 bit MODP group	RFC 2409
Group 2	1024 bits MODP group	RFC 2409
Group 3	EC2N group on GP(2^155)	RFC 2409
Group 4	EC2N group on GP(2^185)	RFC 2409
Group 5	1536 bits MODP group	RFC 3526

Creating a New IPSEC Peer



- Allow this peer to establish SA for non-existing policies. Such policies are created dynamically for the lifetime of SA. Automatic policies allows, for example, to create IPsec secured L2TP tunnels, or any other setup where remote peer's IP address is not known at the configuration time.no - do not generate policies
  - port-override -- generate policies and force policy to use **any** port (old behavior)
  - port-strict -- use ports from peer's proposal, which should match peer's policy
- Phase 1 lifetime: specifies how long the SA will be valid.
- Phase 1 lifetime: specifies how much bytes can be transferred before SA is discarded. If set to **0**, SA will not be discarded due to byte count excess.

Creating a New IPSEC Peer

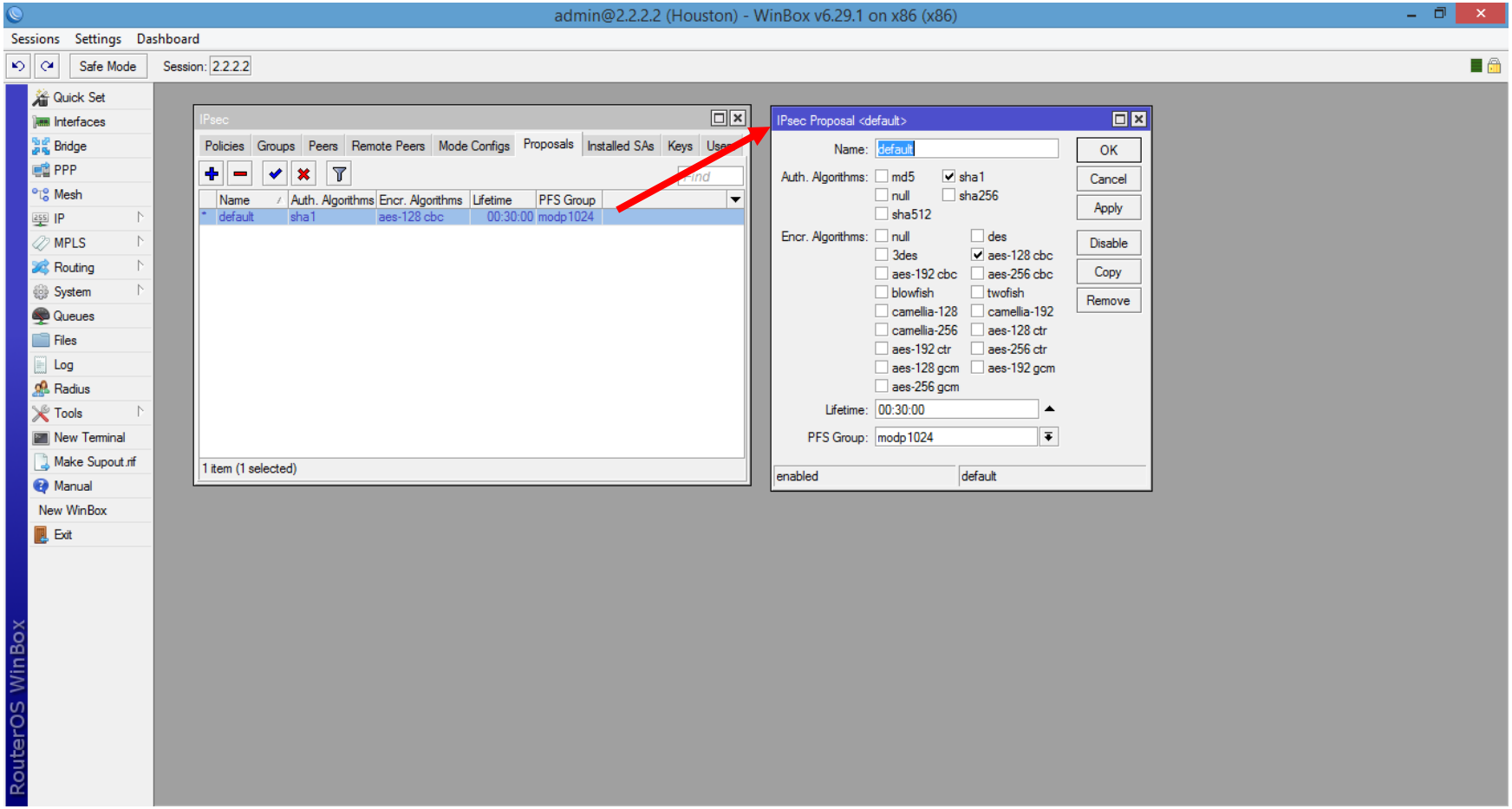


- Dead peer detection interval. If set to disable-dpd, dead peer detection will not be used.
- Maximum count of failures until peer is considered to be dead.

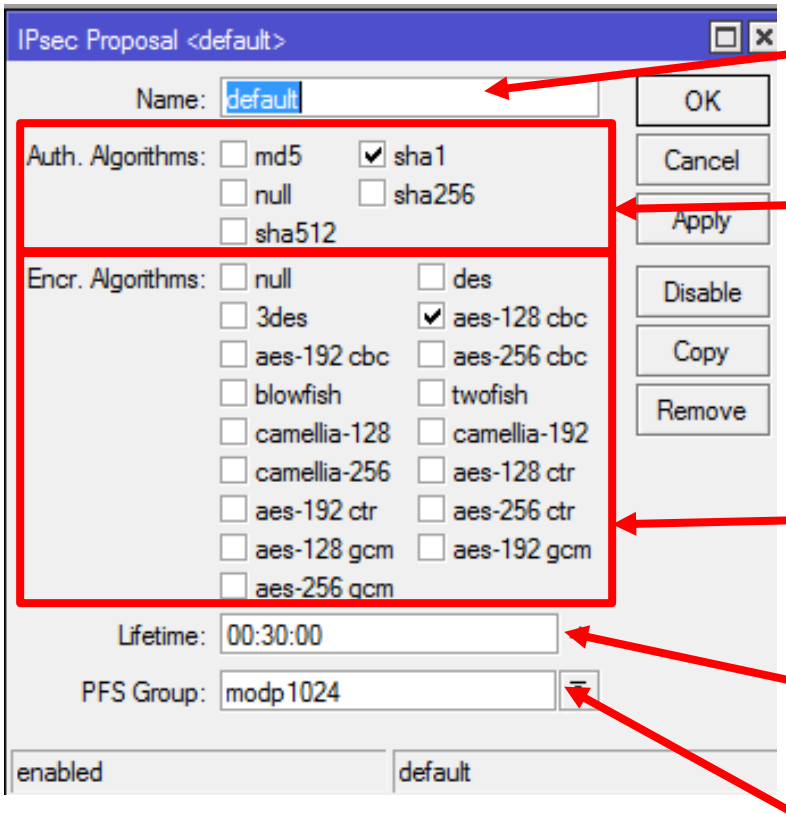
IKE Phase 2

- **Phase 2 -** The peers establish one or more SAs that will be used by IPsec to encrypt data. All SAs established by IKE daemon will have lifetime values (either limiting time, after which SA will become invalid, or amount of data that can be encrypted by this SA, or both). This phase should match following settings:
  - Ipsec protocol
  - mode (tunnel or transport)
  - authentication method
  - PFS (DH) group
  - lifetime

IKE Phase 2 Settings



IKE Phase 2 Settings



- Name of the proposal template.
- Allowed algorithms for authorization. sha1 is stronger, but slower algorithm.
- Allowed algorithms and key lengths to use for SAs.
- How long to use SA before throwing it out.
- Diffie-Helman group used for Perfect Forward Secrecy.

IPSEC

- Once the tunnel configuration is set you have to generate "interesting traffic" before the tunnel will establish.
- Check the Remote Peers and Installed SAs Tabs to verify tunnel is running.
- Sometime the routers will need to be rebooted before the tunnel will establish correctly.
- You may want to add the "IPSEC" topic to the logging rules to help troubleshoot.

End of Module