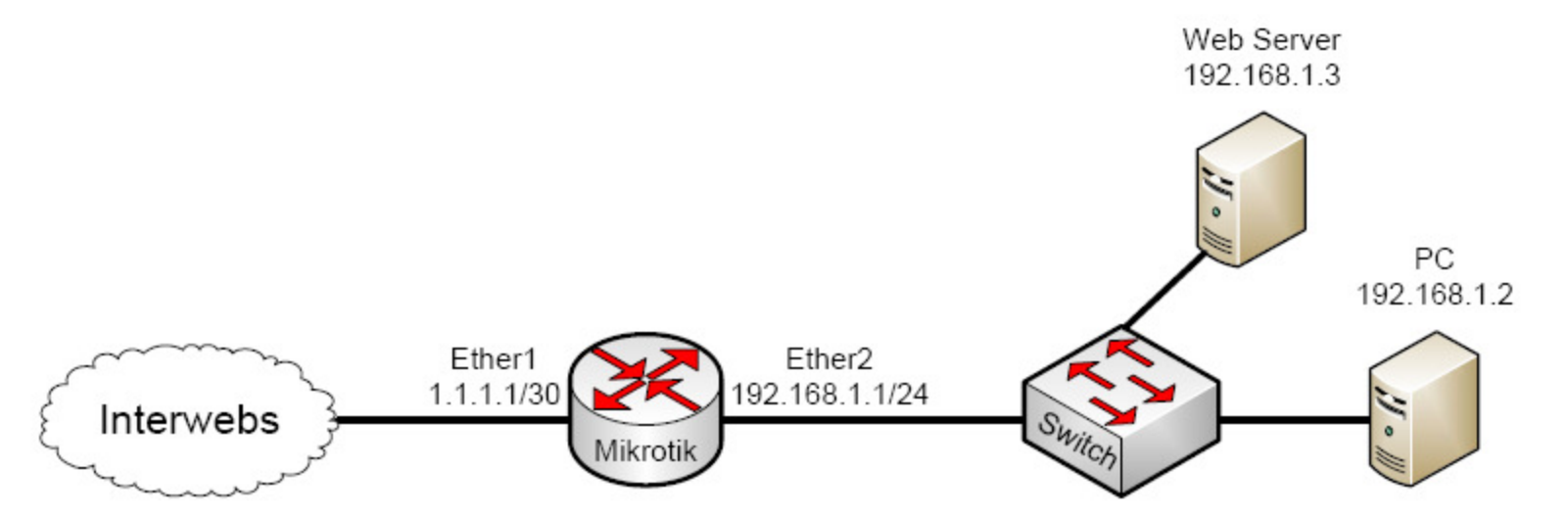
<3G Networks>

Mikrotik VPN

What is a VPN

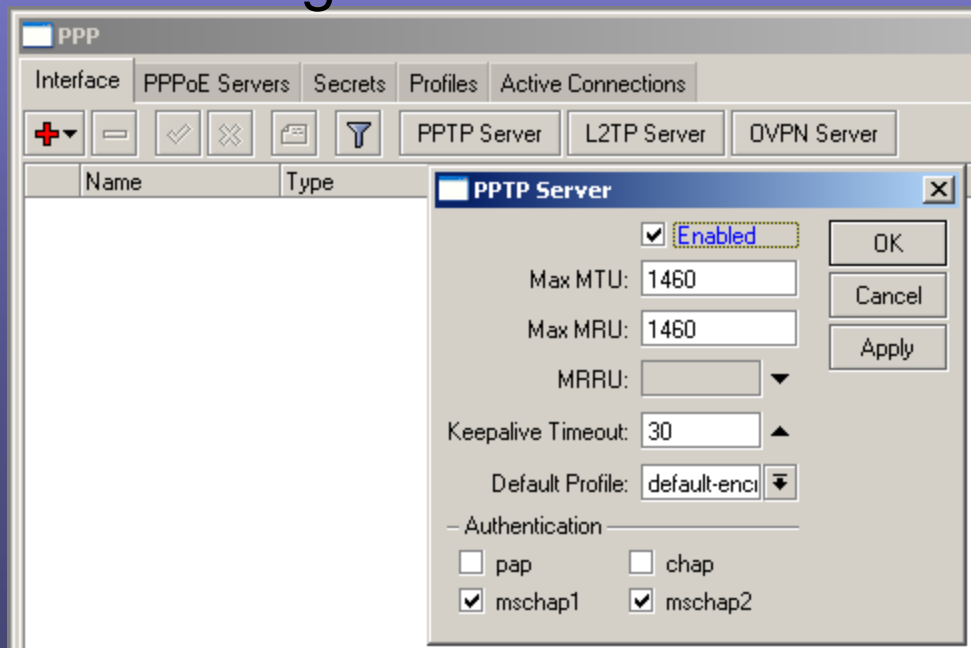
- Wikipedia has a very lengthy explanation http://en.wikipedia.org/wiki/Virtual_private_network
- This class is really going to deal with tunneling network traffic over IP both securely and not so securely.

Basic Diagram



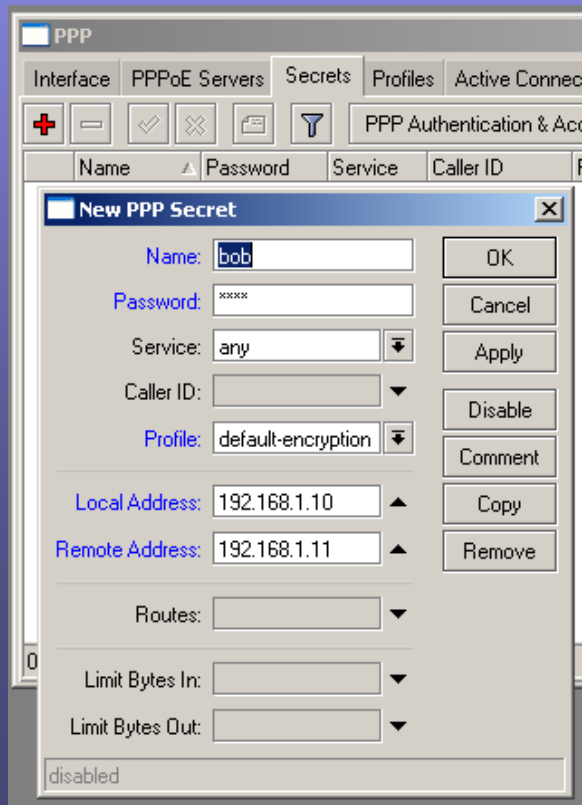
PPTP – Point to Point Tunneling Protocol

- PPTP tunnels ALL traffic through the PPTP server. There is no “split tunneling” option. You can’t pass any options back to the client other than an IP.
- Easy option for client connections. Every modern Windows OS will have built in PPTP client.
- PPTP offers NO encryption if not using MSCHAP V2.
- Enabling PPTP for remote:
  - Go to PPP
  - Choose PPTP server
  - Check enable and click OK



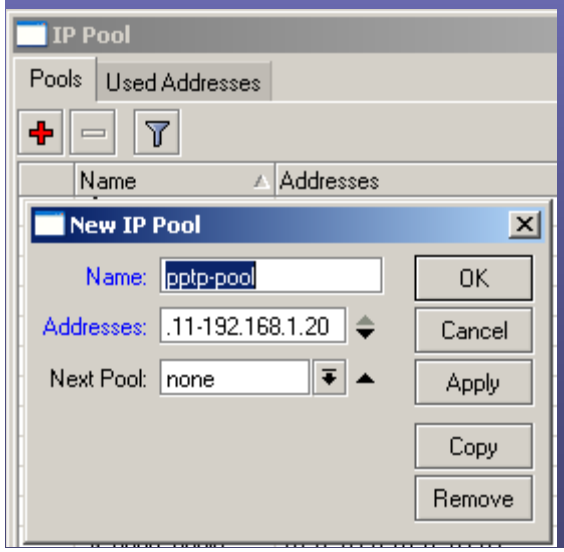
PPTP Secret

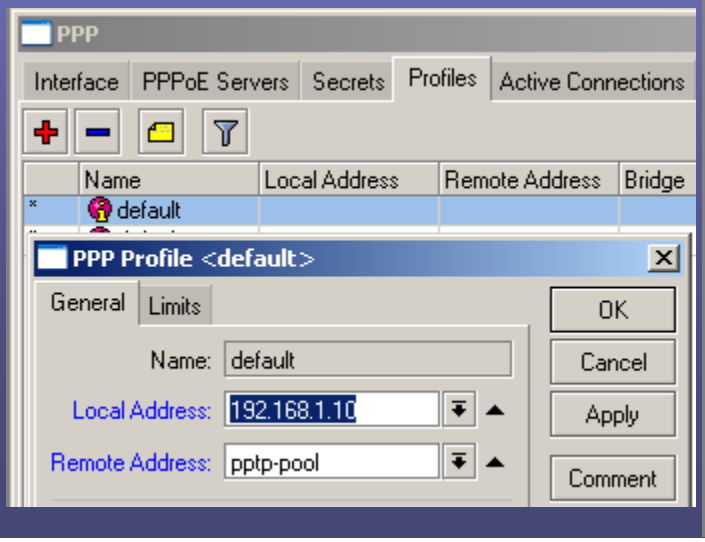
- Adding a user can be done via the secrets tab.
- Name is login username
- Password
- Local address can be same for all of the users.
- Remote address must be unique for all users.

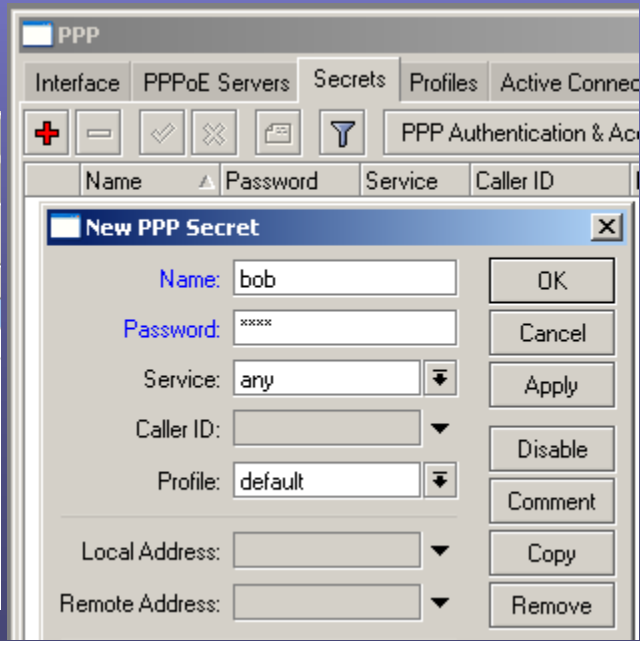


PPTP with Pool IP Assignment

- Create a pool of addresses: IP -> Pool
- Edit PPP Profile and add the new pool for remotes and add local IP all will use.
- Create secret sans local and remote.

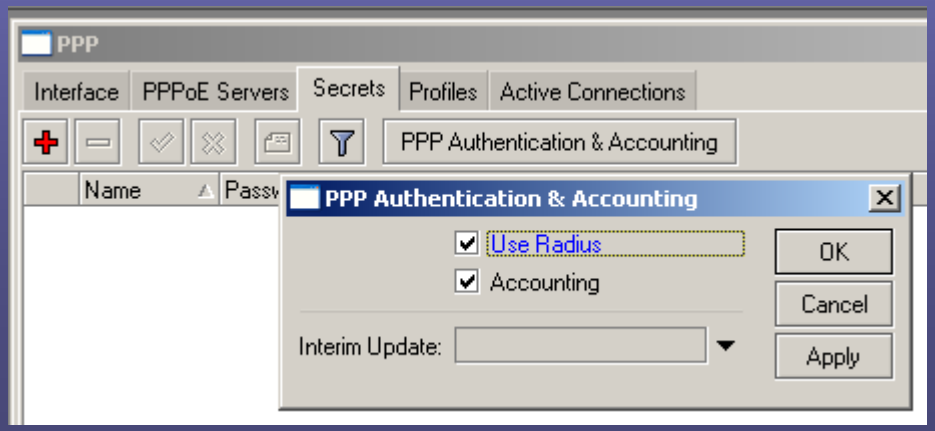






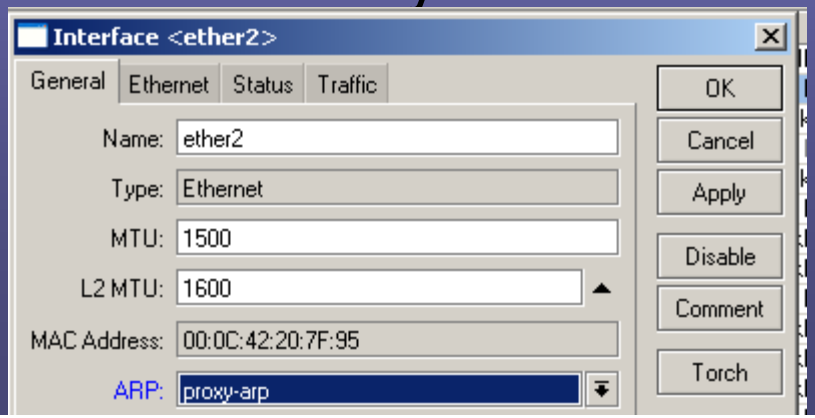
PPTP with Radius

- Under secrets, click PPP Authentication & Accounting.
- Check “use radius”.



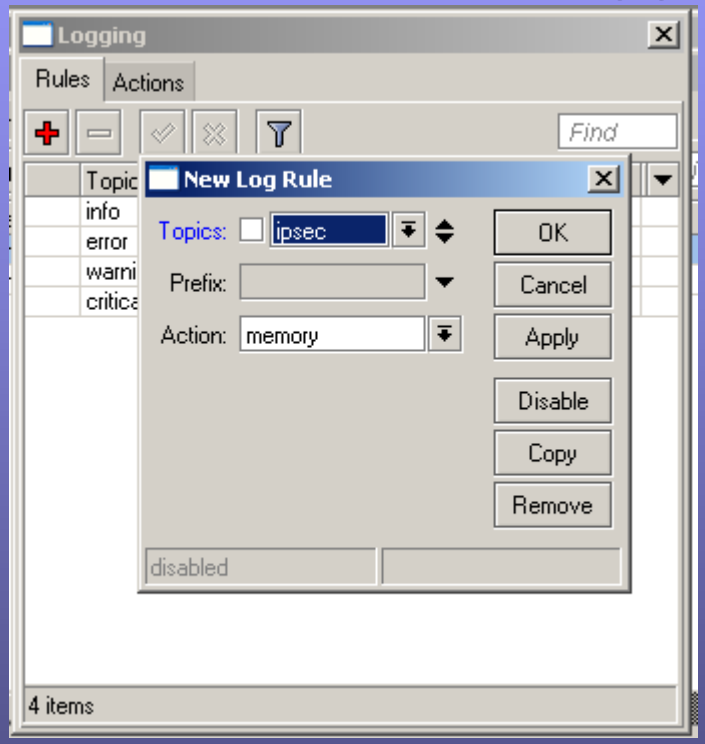
PPTP and Proxy-ARP

- Looking at our basic diagram and using the config shown above, you will most likely need to enable proxy arp on the ether2 interface.
- This is due to the fact that we have PPTP clients terminating on the router using the same subnet as the ether2 interface.
- When a user connects via PPTP it creates a PPTP interface, so if the user wants to be able to properly communicate with the ether2 interface they need their ARP packets to traverse the router to and from the ether2 interface to the newly created PPTP interface.

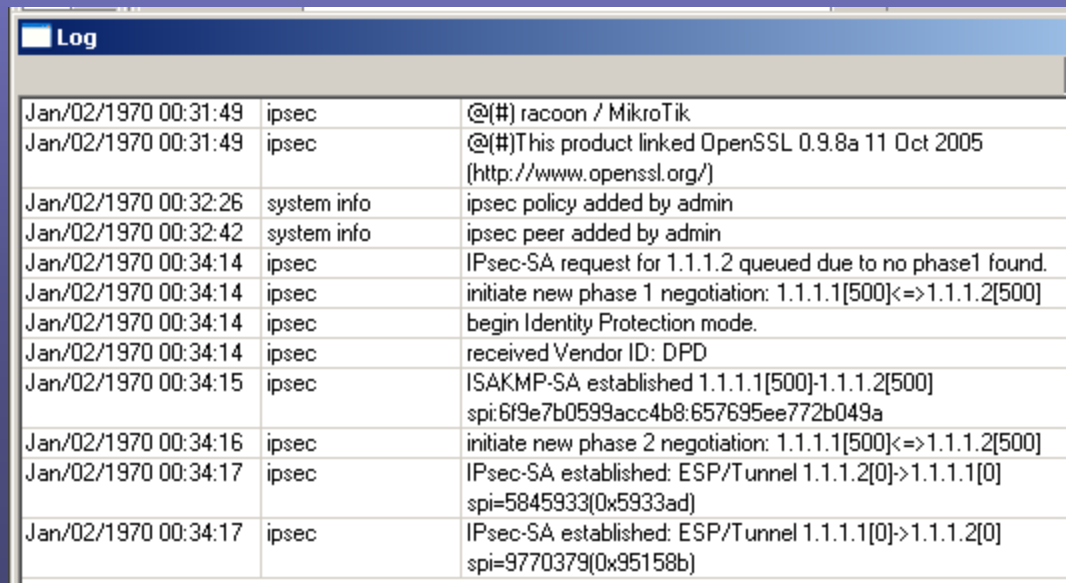


IPSec Logging

- Enable IPSec logging. System -> Logging



- View Log ->



Log

Jan/02/1970 00:31:49	ipsec	@(#) racoon / MikroTik
Jan/02/1970 00:31:49	ipsec	@(#)This product linked OpenSSL 0.9.8a 11 Oct 2005 (http://www.openssl.org/)
Jan/02/1970 00:32:26	system info	ipsec policy added by admin
Jan/02/1970 00:32:42	system info	ipsec peer added by admin
Jan/02/1970 00:34:14	ipsec	IPsec-SA request for 1.1.1.2 queued due to no phase1 found.
Jan/02/1970 00:34:14	ipsec	initiate new phase 1 negotiation: 1.1.1.1[500]<=>1.1.1.2[500]
Jan/02/1970 00:34:14	ipsec	begin Identity Protection mode.
Jan/02/1970 00:34:14	ipsec	received Vendor ID: DPD
Jan/02/1970 00:34:15	ipsec	ISAKMP-SA established 1.1.1.1[500]-1.1.1.2[500] spi:6f9e7b0599acc4b8:657695ee772b049a
Jan/02/1970 00:34:16	ipsec	initiate new phase 2 negotiation: 1.1.1.1[500]<=>1.1.1.2[500]
Jan/02/1970 00:34:17	ipsec	IPsec-SA established: ESP/Tunnel 1.1.1.2[0]->1.1.1.1[0] spi=5845933(0x5933ad)
Jan/02/1970 00:34:17	ipsec	IPsec-SA established: ESP/Tunnel 1.1.1.1[0]->1.1.1.2[0] spi=9770379(0x95158b)

IPSec

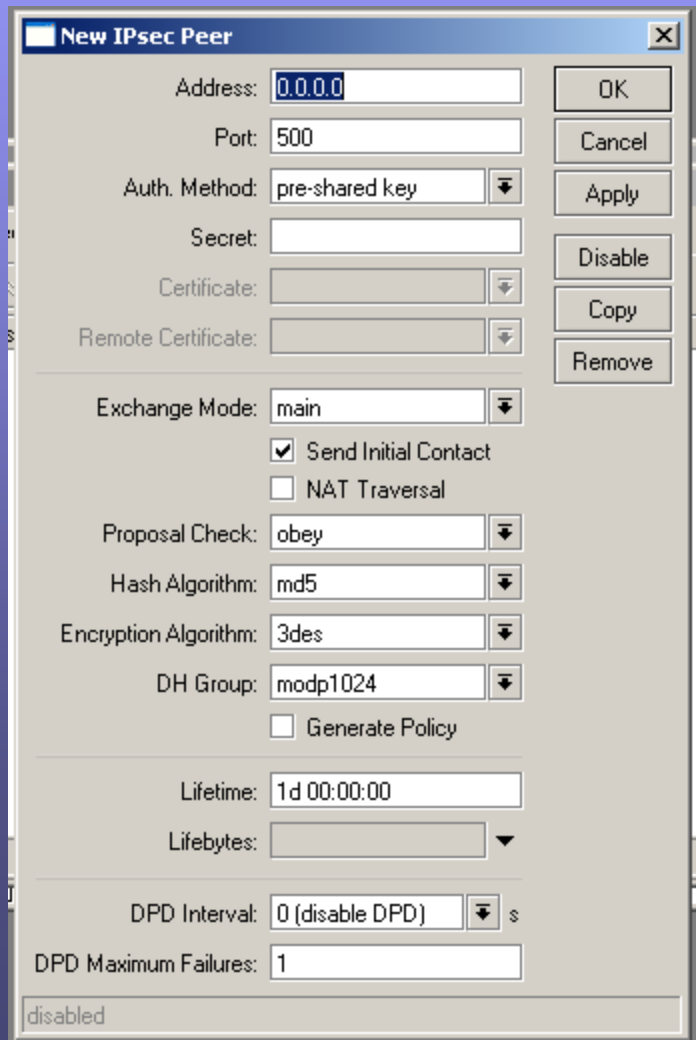
- Two methods to be demonstrated:
  - IPSec Tunnel Mode
  - IPSec Transport w/IPIP tunnel
- IPSec Tunnel mode
  - Uses fewer system resources on router
  - Single layer of complexity
- IPSec Transport w/IPIP tunnel
  - Creates an IPIP tunnel then uses IPSec to encrypt IPIP traffic
  - Uses more system resources
  - Increases complexity
  - Allows for dynamic routing protocols
  - Allows for multicast traffic to be passed
  - Allows for multiple WAN connection failover

IPSec

- 3 parts to creating IPSec connection
  - Peer (Phase 1)
  - Policy (Phase 2)
  - Proposal (Transform set)

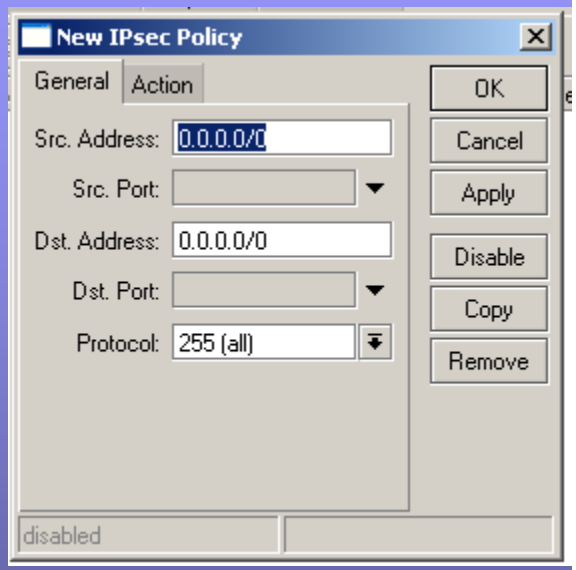
IPSec - Peer

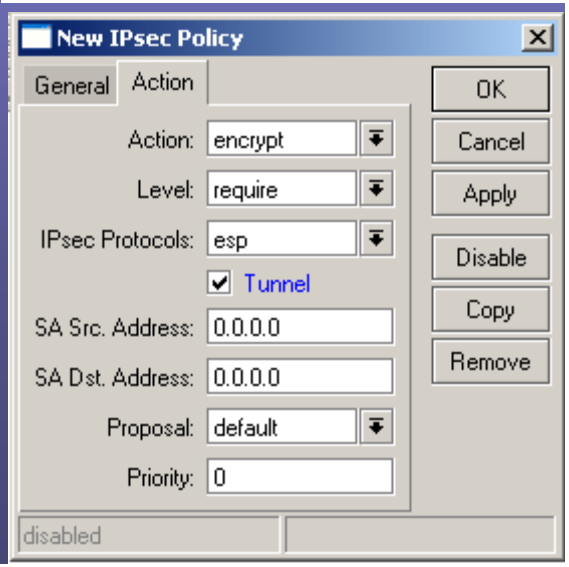
- Peer specifies phase 1 security.
- Make them match on both sides.



IPSec - Policy

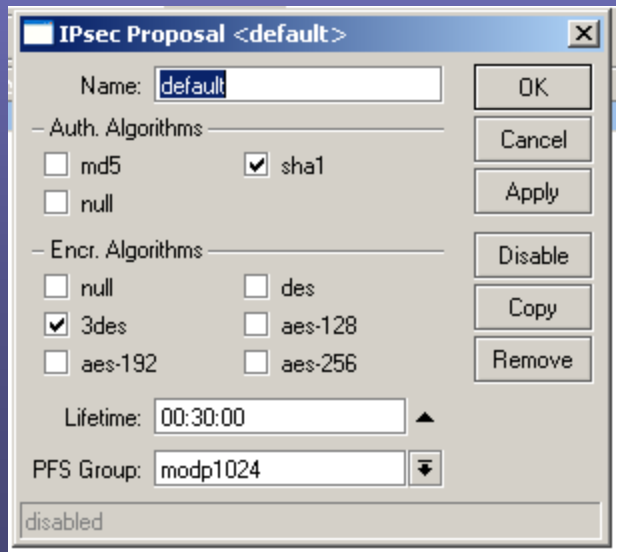
- Peer specifies phase 2 security.
- Make the settings match on both sides. IP information in reverse order.



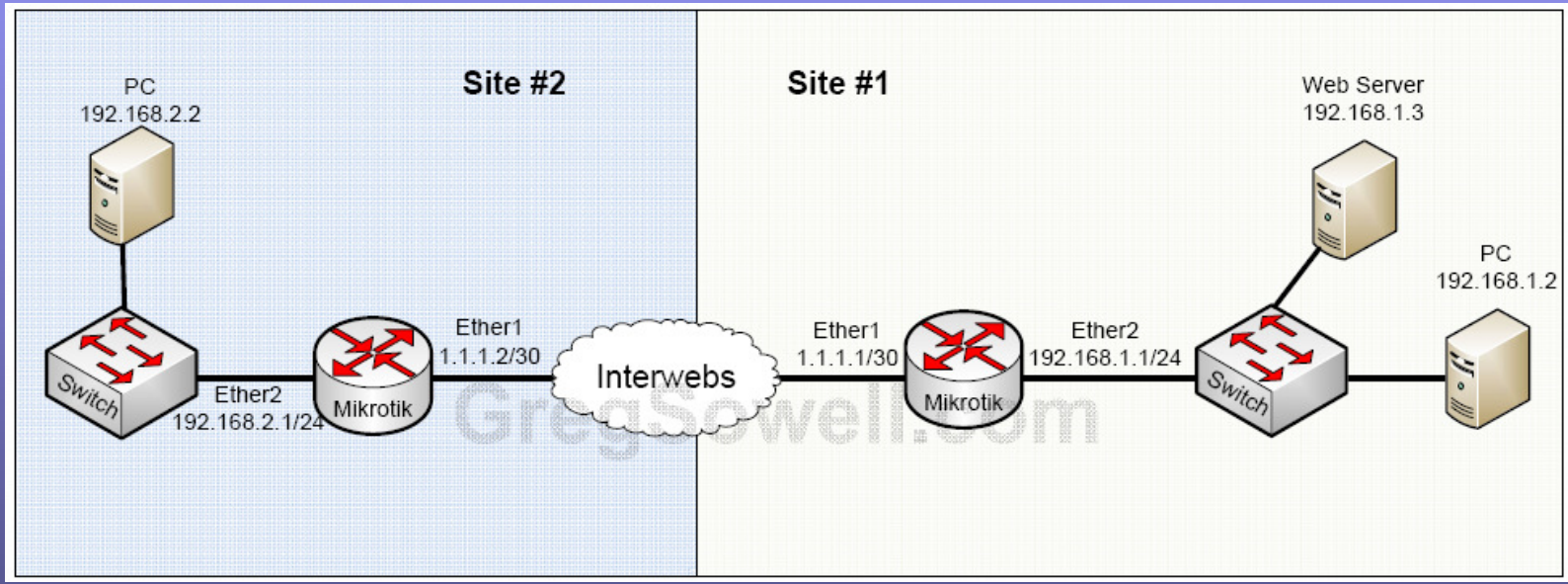


IPSec - Proposal

- Sent by IKE to establish Security Associations (SA). Which algorithms will be used in phase 2.
- Make the settings match on both sides.



IPSec Tunnel – MTK to MTK



IPSec Tunnel – MTK to MTK - Site # 1

Create Peer

New IPsec Peer

Address: 1.1.1.2
Port: 500
Auth. Method: pre-shared key
Secret: test
Certificate:
Remote Certificate:
Exchange Mode: main
☑ Send Initial Contact
☐ NAT Traversal
Proposal Check: obey
Hash Algorithm: md5
Encryption Algorithm: 3des
DH Group: modp1024
☐ Generate Policy
Lifetime: 1d 00:00:00
Lifebytes:
DPD Interval: 0 (disable DPD) s
DPD Maximum Failures: 1

OK | Cancel | Apply | Disable | Copy | Remove

disabled

Create Policy

New IPsec Policy

General | Action

Src. Address: 192.168.1.0/24
Src. Port:
Dst. Address: 192.168.2.0/24
Dst. Port:
Protocol: 255 (all)

OK | Cancel | Apply | Disable | Copy | Remove

New IPsec Policy

General | Action

Action: encrypt
Level: require
IPsec Protocols: esp
☑ Tunnel
SA Src. Address: 1.1.1.1
SA Dst. Address: 1.1.1.2
Proposal: default
Priority: 0

OK | Cancel | Apply | Disable | Copy | Remove

disabled

Create/Modify Proposal if you choose

IPsec Proposal <default>

Name: default

– Auth. Algorithms
☐ md5 ☑ sha1
☐ null

– Encr. Algorithms
☐ null ☐ des
☑ 3des ☐ aes-128
☐ aes-192 ☐ aes-256

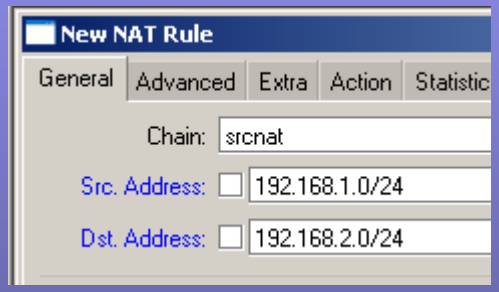
Lifetime: 00:30:00
PFS Group: modp1024

OK | Cancel | Apply | Disable | Copy | Remove

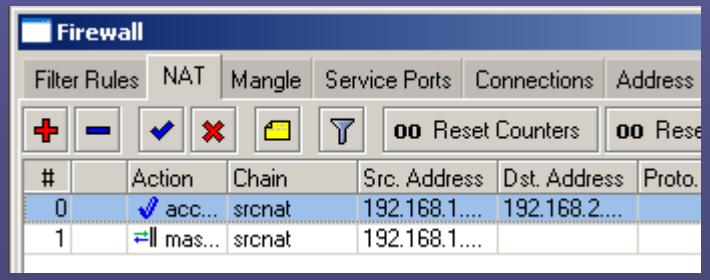
disabled

IPSec Tunnel – MTK to MTK - Site # 1

- IP -> Firewall -> NAT
- Create NAT bypass for traffic that should traverse the tunnel.



- Move the rule to the top.



IPSec Tunnel – MTK to MTK - Site # 2

Create Peer

New IPsec Peer

Address: 1.1.1.1
Port: 500
Auth. Method: pre-shared key
Secret: test
Certificate:
Remote Certificate:
Exchange Mode: main
☑ Send Initial Contact
☐ NAT Traversal
Proposal Check: obey
Hash Algorithm: md5
Encryption Algorithm: 3des
DH Group: modp1024
☐ Generate Policy
Lifetime: 1d 00:00:00
Lifebytes:
DPD Interval: 0 (disable DPD) s
DPD Maximum Failures: 1

OK | Cancel | Apply | Disable | Copy | Remove

disabled

Create Policy

New IPsec Policy

General | Action

Src. Address: 192.168.2.0/24
Src. Port:
Dst. Address: 192.168.1.0/24
Dst. Port:
Protocol: 255 (all)

OK | Cancel | Apply | Disable | Copy | Remove

New IPsec Policy

General | Action

Action: encrypt
Level: require
IPsec Protocols: esp
☑ Tunnel
SA Src. Address: 1.1.1.2
SA Dst. Address: 1.1.1.1
Proposal: default
Priority: 0

OK | Cancel | Apply | Disable | Copy | Remove

disabled

Create/Modify

Proposal if you choose

IPsec Proposal <default>

Name: default

– Auth. Algorithms
☐ md5 ☑ sha1
☐ null

– Encr. Algorithms
☐ null ☐ des
☑ 3des ☐ aes-128
☐ aes-192 ☐ aes-256

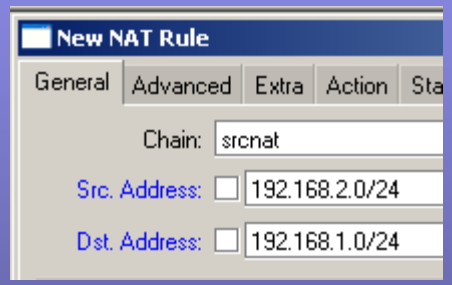
Lifetime: 00:30:00
PFS Group: modp1024

OK | Cancel | Apply | Disable | Copy | Remove

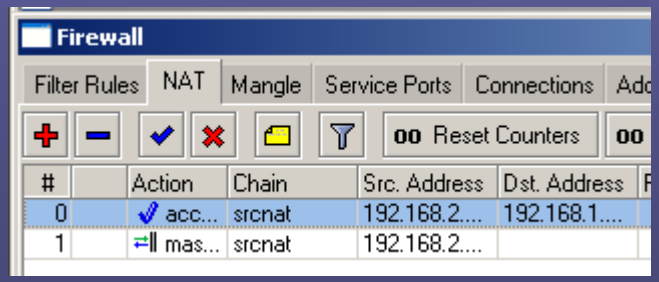
disabled

IPSec Tunnel – MTK to MTK - Site # 2

- IP -> Firewall -> NAT
- Create NAT bypass for traffic that should traverse the tunnel.

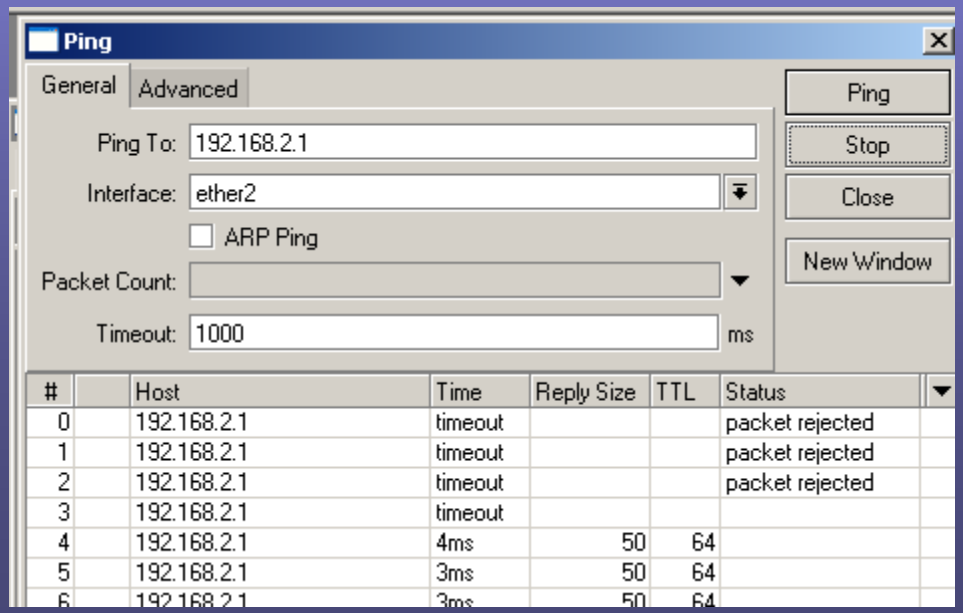


- Move the rule to the top.

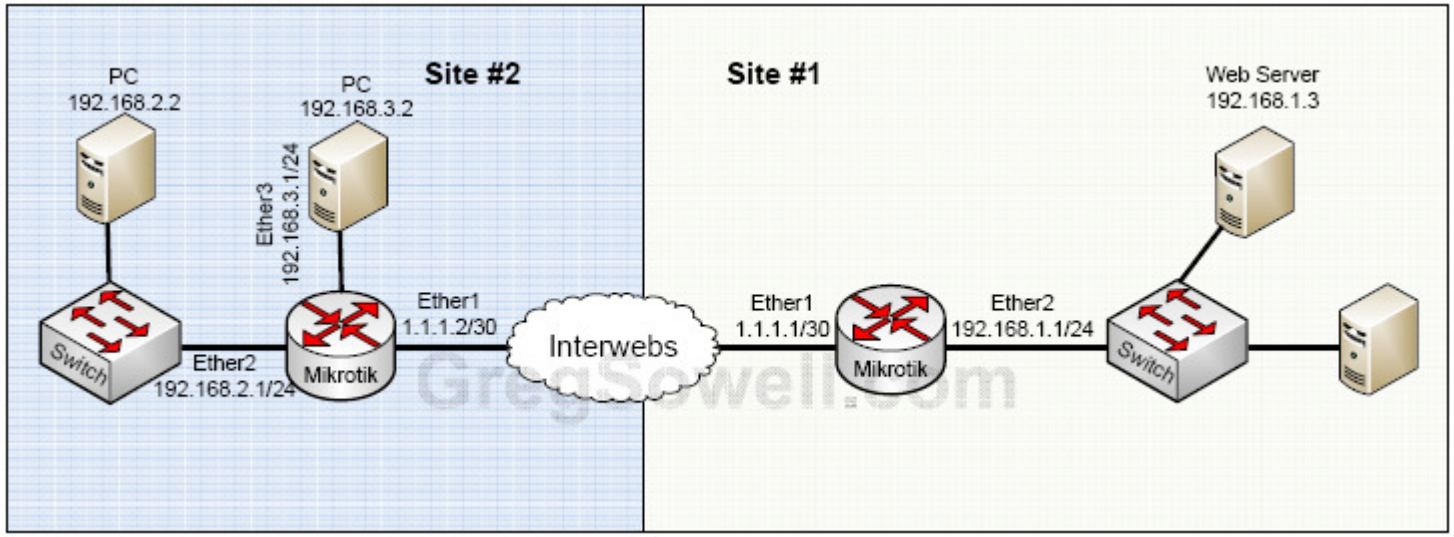


IPSec Interesting Traffic

- “Interesting Traffic” is traffic that is specified in a policy and should be encrypted.
- To test our tunnel from the router use the ping tool and specify the interface as the inside interface(192.168.1.1). This will source the pings from 192.168.1.1 and thus will be considered interesting. This will then attempt to traverse the tunnel.



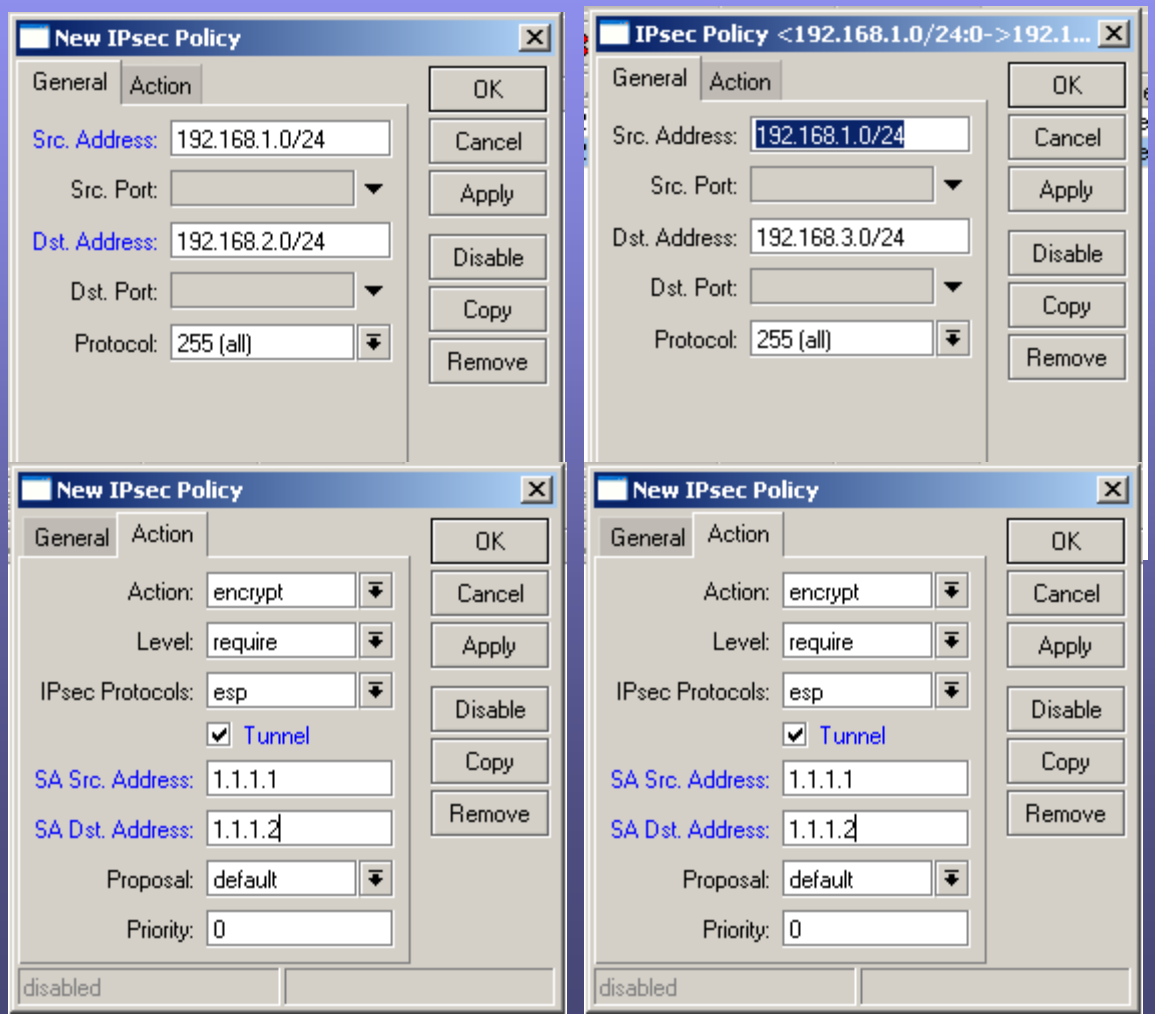
IPSec Tunnel – MTK to MTK Multiple Subnets



IPSec Tunnel – MTK to MTK - Site # 1

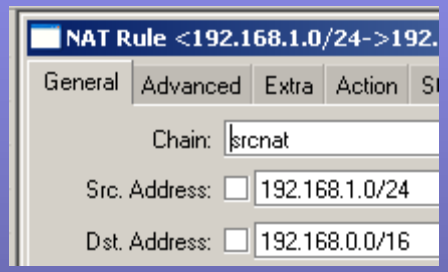
Create Peer/ Proposal same as above

Create Policies

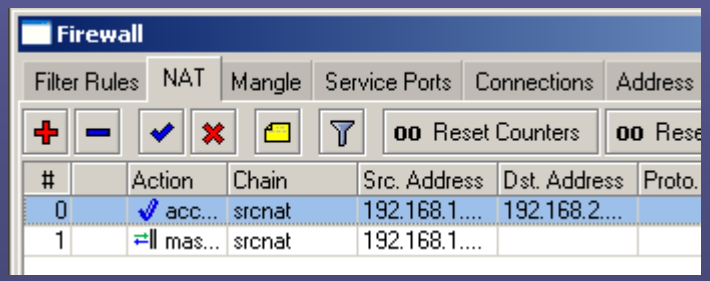


IPSec Tunnel – MTK to MTK - Site # 1

- IP -> Firewall -> NAT
- Create NAT bypass for traffic that should traverse the tunnel.



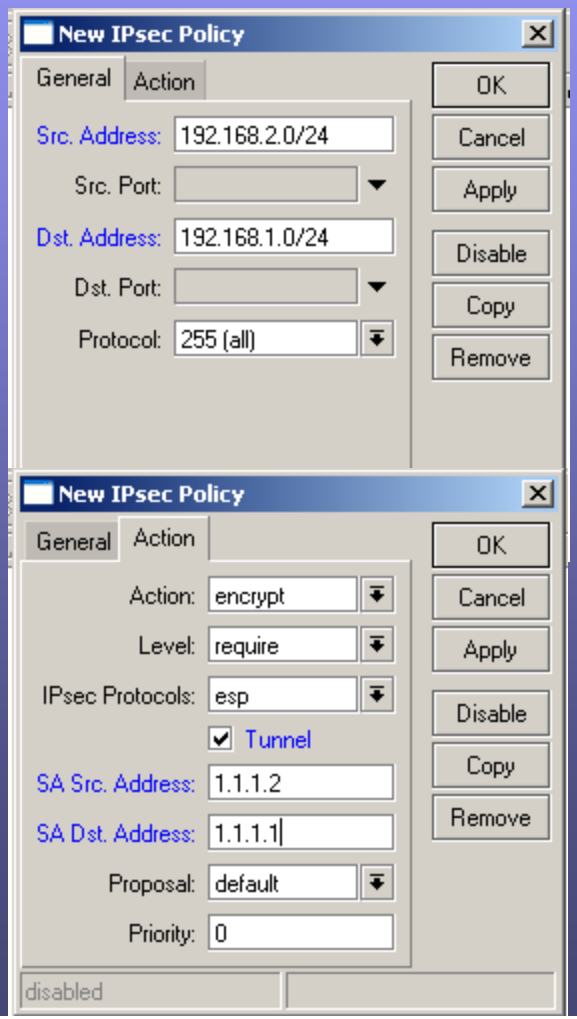
- Move the rule to the top.

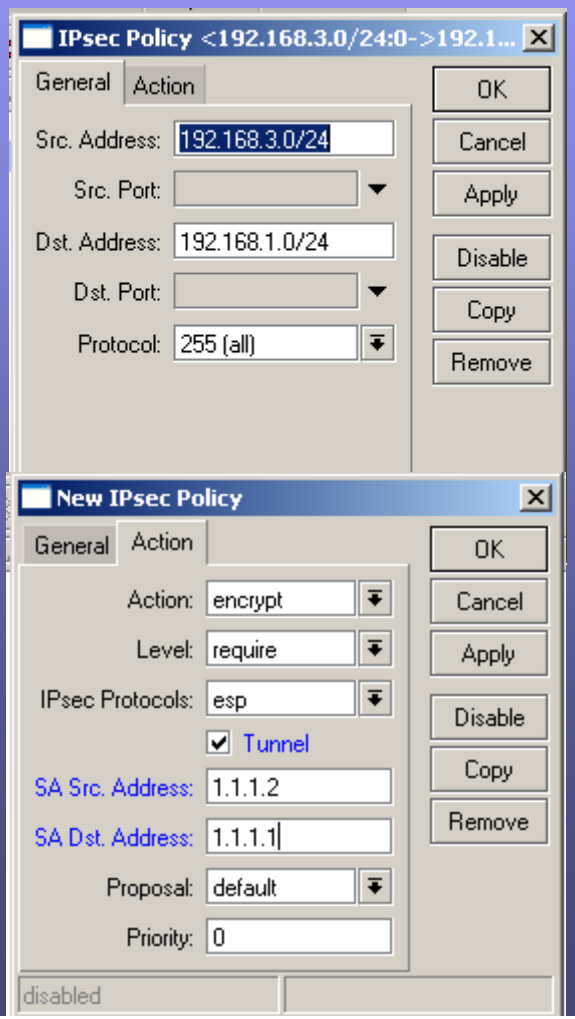


IPSec Tunnel – MTK to MTK - Site # 2

Create Peer/Proposal same as above

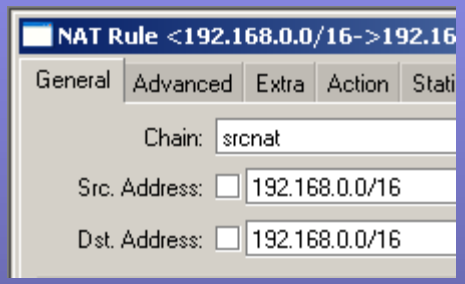
Create Policies



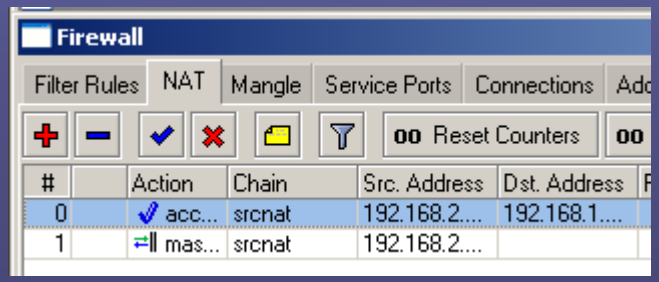


IPSec Tunnel – MTK to MTK - Site # 2

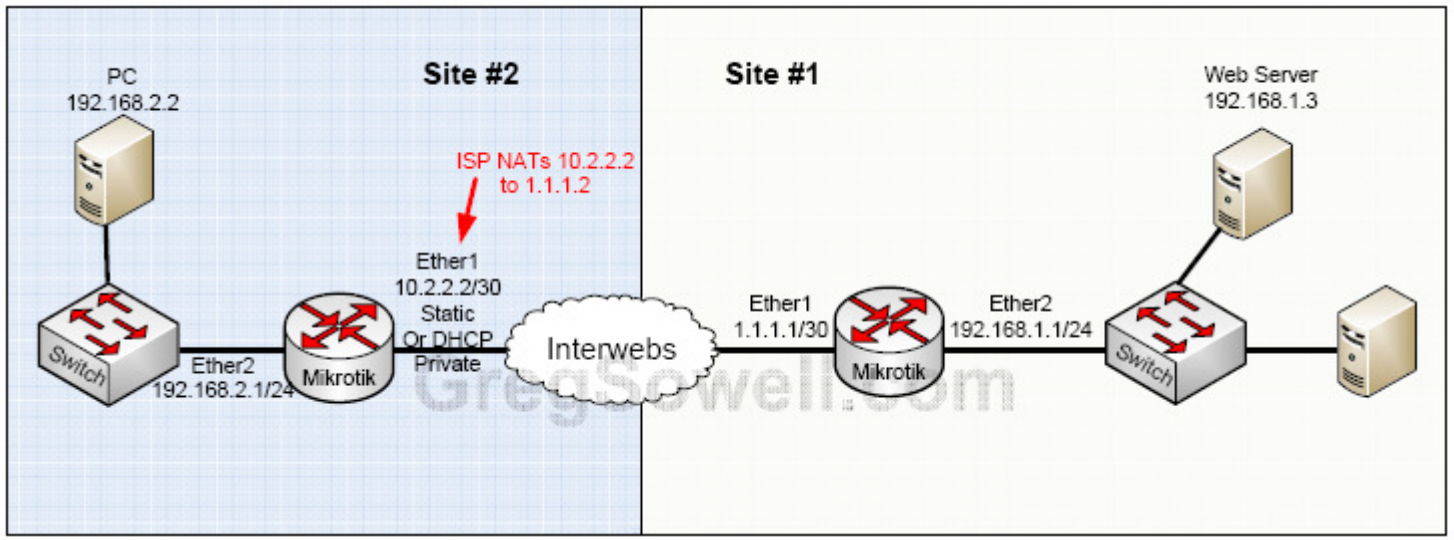
- IP -> Firewall -> NAT
- Create NAT bypass for traffic that should traverse the tunnel.



- Move the rule to the top.

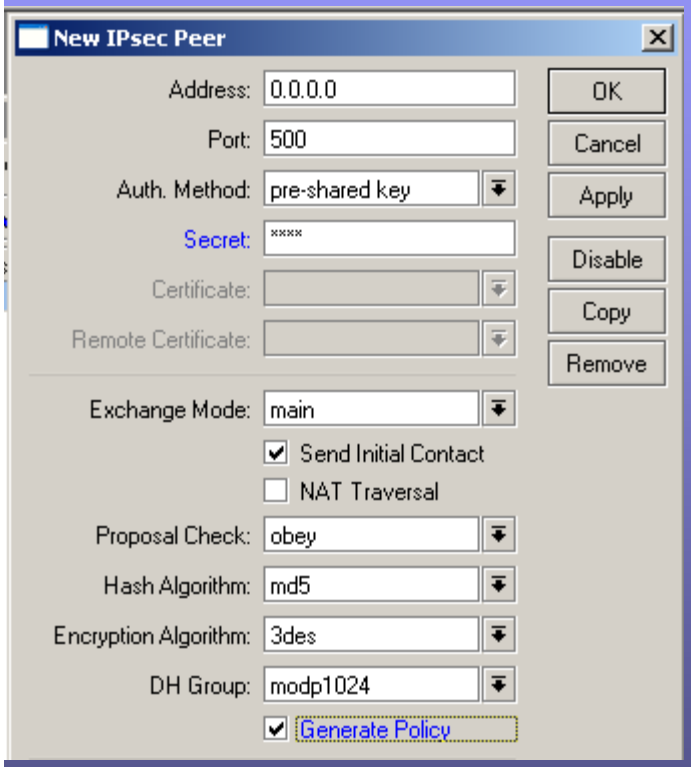


IPSec Tunnel – MTK to MTK One Site has Private WAN IP



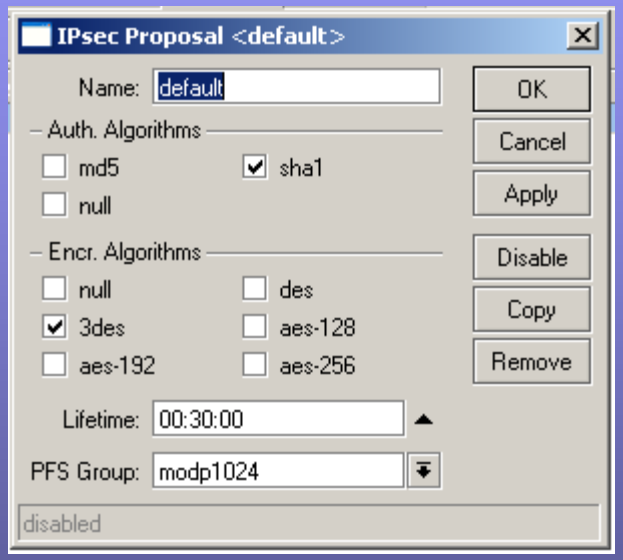
IPSec Tunnel – MTK to MTK - Site # 1

Create Peer



Create/Modify

Proposal if you choose

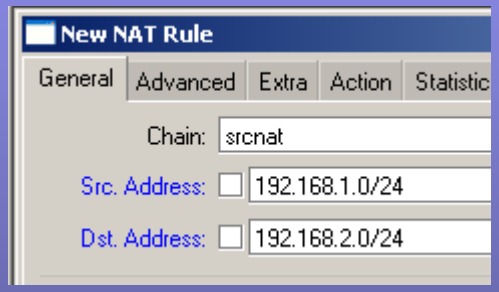


Set IP to 0.0.0.0 (Any remote Peer).

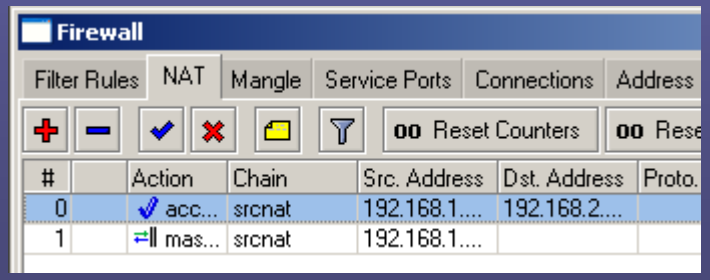
Check Generate Policy.

IPSec Tunnel – MTK to MTK - Site # 1

- IP -> Firewall -> NAT
- Create NAT bypass for traffic that should traverse the tunnel.



- Move the rule to the top.



IPSec Tunnel – MTK to MTK - Site # 2

Create Peer

New IPsec Peer

Address: 1.1.1.1
Port: 500
Auth. Method: pre-shared key
Secret: test
Certificate:
Remote Certificate:
Exchange Mode: main
☑ Send Initial Contact
☐ NAT Traversal
Proposal Check: obey
Hash Algorithm: md5
Encryption Algorithm: 3des
DH Group: modp1024
☐ Generate Policy
Lifetime: 1d 00:00:00
Lifebytes:
DPD Interval: 0 (disable DPD) s
DPD Maximum Failures: 1

OK | Cancel | Apply | Disable | Copy | Remove

disabled

Create Policy

New IPsec Policy

General | Action

Src. Address: 192.168.2.0/24
Src. Port:
Dst. Address: 192.168.1.0/24
Dst. Port:
Protocol: 255 (all)

OK | Cancel | Apply | Disable | Copy | Remove

IPsec Policy <192.168.2.0/24:0->192.1...

General | Action

Action: encrypt
Level: require
IPsec Protocols: esp
☑ Tunnel
SA Src. Address: 10.2.2.2
SA Dst. Address: 1.1.1.1
Proposal: default
Priority: 0

OK | Cancel | Apply | Disable | Copy | Remove

disabled

Create/Modify Proposal if you choose

IPsec Proposal <default>

Name: default

Auth. Algorithms
☐ md5 ☑ sha1
☐ null

Encr. Algorithms
☐ null ☐ des
☑ 3des ☐ aes-128
☐ aes-192 ☐ aes-256

Lifetime: 00:30:00
PFS Group: modp1024

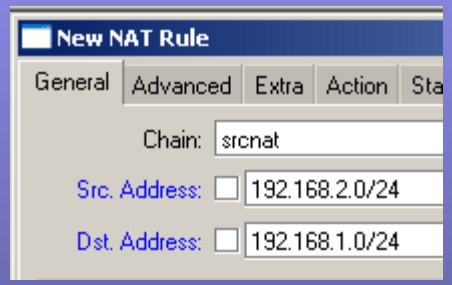
OK | Cancel | Apply | Disable | Copy | Remove

disabled

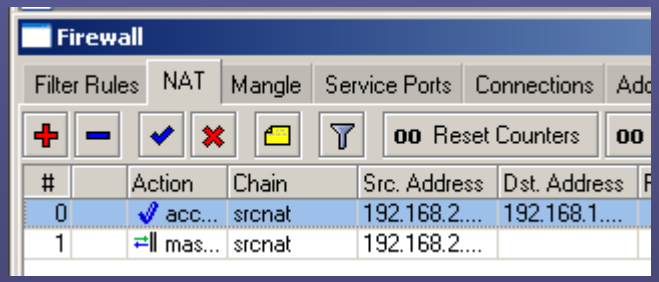
<= Set SA Src Address to whatever IP is bound to the WAN interface. Be it private or public even if it is later NAT'd.

IPSec Tunnel – MTK to MTK - Site # 2

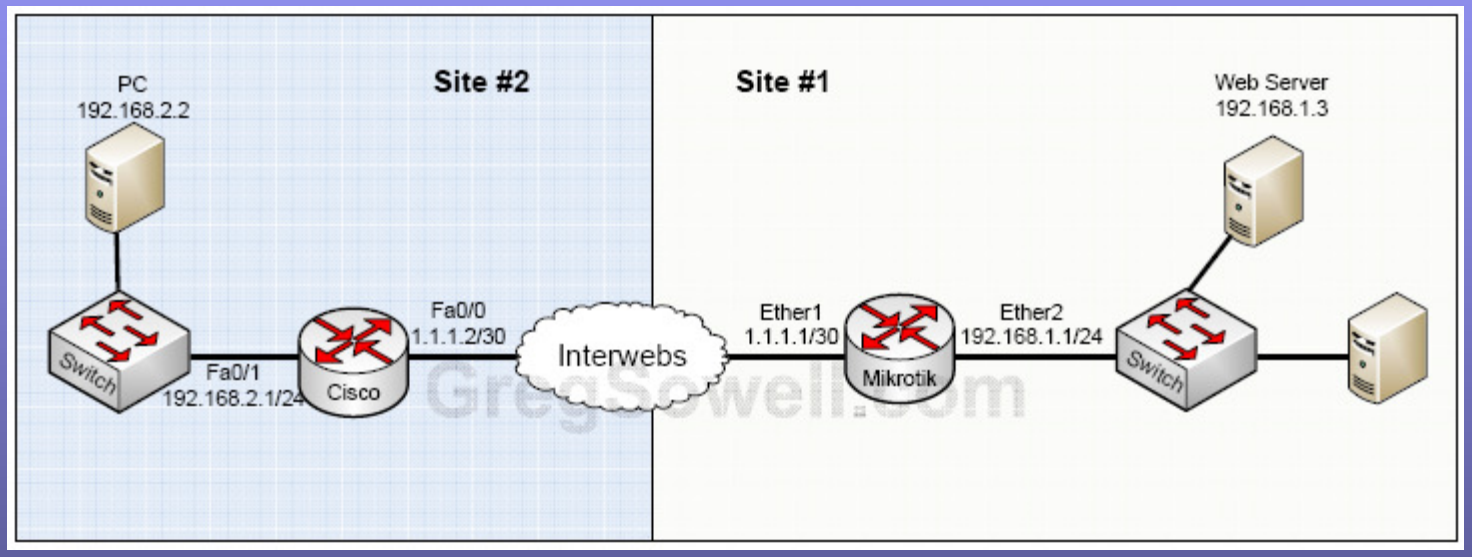
- IP -> Firewall -> NAT
- Create NAT bypass for traffic that should traverse the tunnel.



- Move the rule to the top.

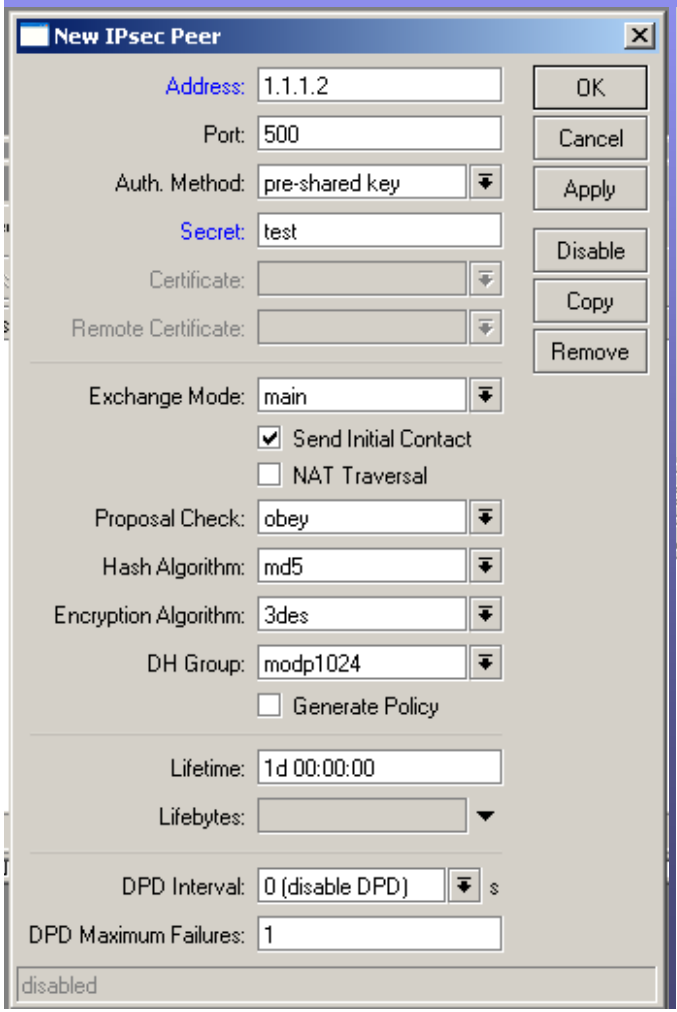


IPSec Tunnel – MTK to Cisco Router/ASA

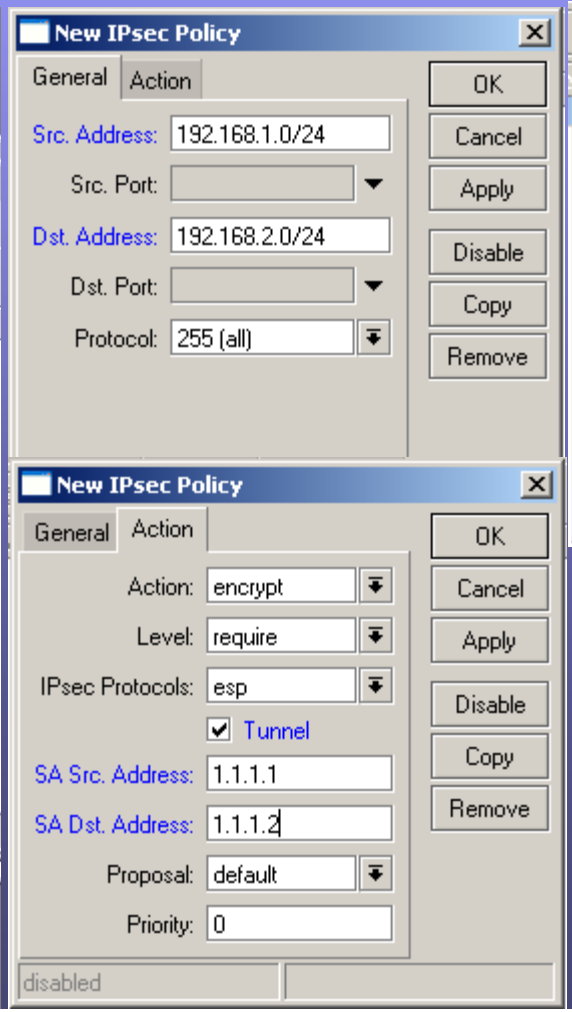


IPSec Tunnel – MTK to Cisco RTR - Site # 1

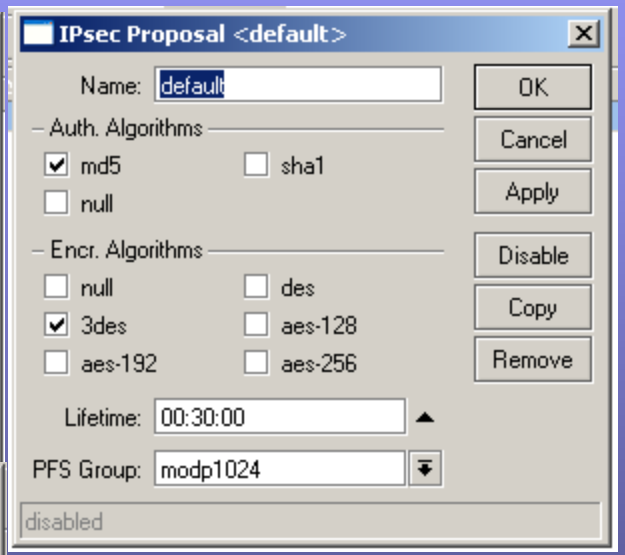
Create Peer



Create Policy



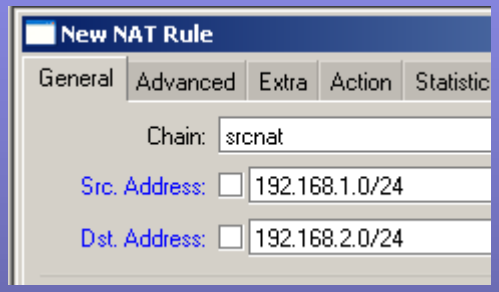
Create/Modify proposal if you



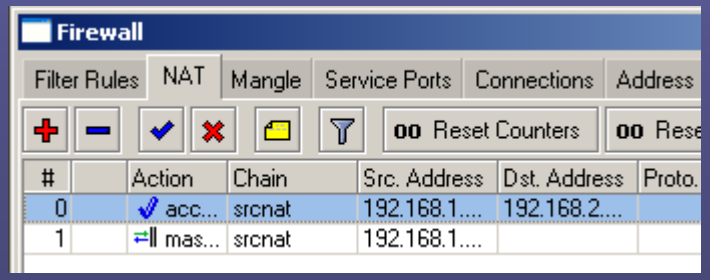
I changed the proposal to use MD5

IPSec Tunnel – MTK to MTK - Site # 1

- IP -> Firewall -> NAT
- Create NAT bypass for traffic that should traverse the tunnel.



- Move the rule to the top.



IPSec Tunnel – MTK to Cisco RTR - Site # 2

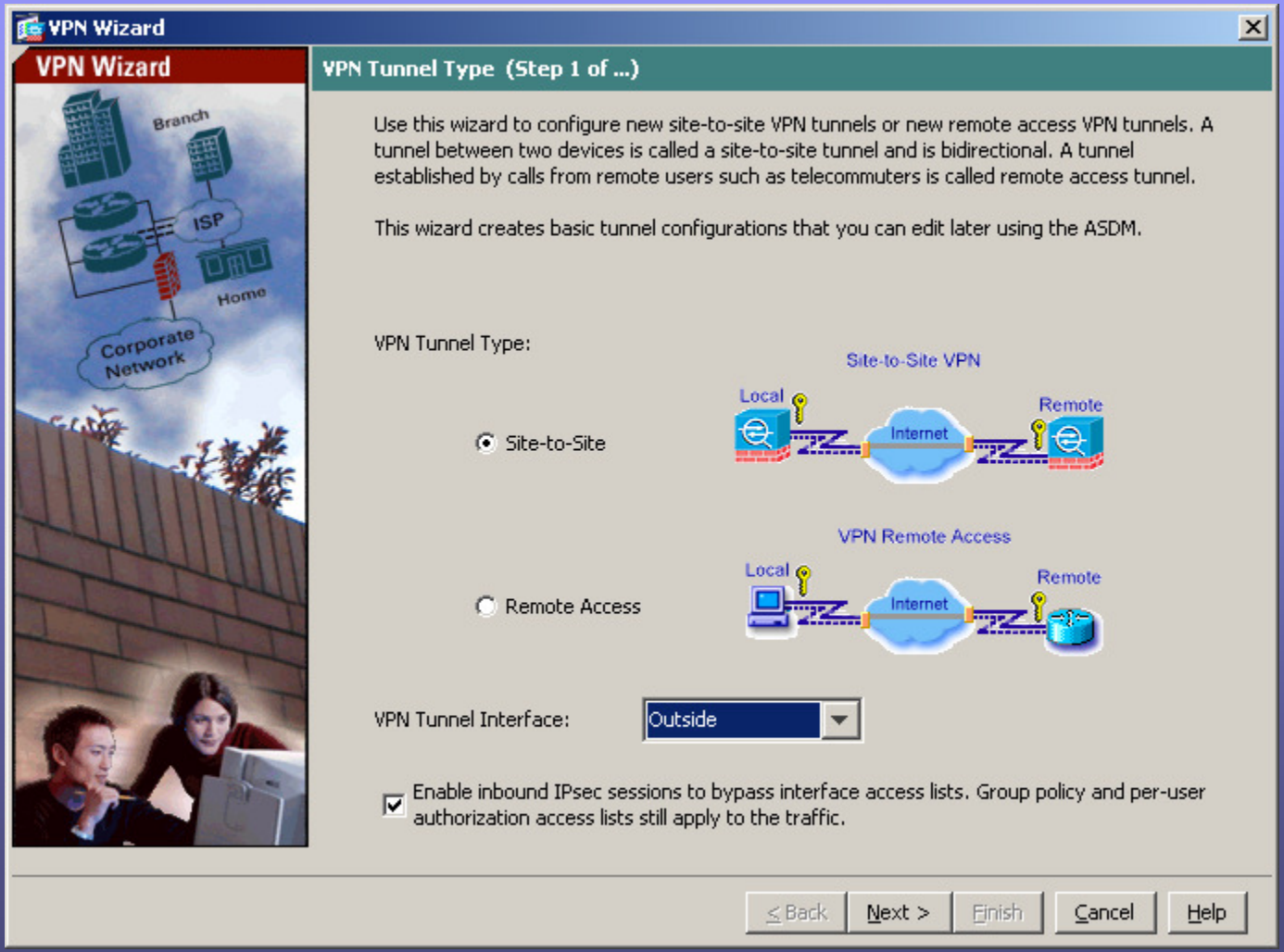
```
crypto isakmp policy 1
 hash md5
 encr 3des
 authentication pre-share
 group 2
 lifetime 14400

crypto isakmp key test address 1.1.1.1

crypto ipsec transform-set to_remotes esp-3des esp-md5-hmac

crypto map to_remotes 10 ipsec-isakmp
 set pfs group2
 set peer 1.1.1.1
 set transform-set to_remotes
 match address Kitchen

int e0
ip address 1.1.1.2 255.255.255.252
crypto map to_remotes
no shut

int ep1
ip address 192.168.2.1 255.255.255.0
no shut

ip route 0.0.0.0 0.0.0.0 1.1.1.1

ip nat inside source list NAT interface e0 overload

ip access-list extended Kitchen
 remark Allow access though tunnel to Kitchen LAN
 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

ip access-list extended NAT
 deny   ip any 192.168.0.0 0.0.255.255
 permit ip any any
```

IPSec Tunnel –Cisco RTR - Site # 2 Trouble shooting

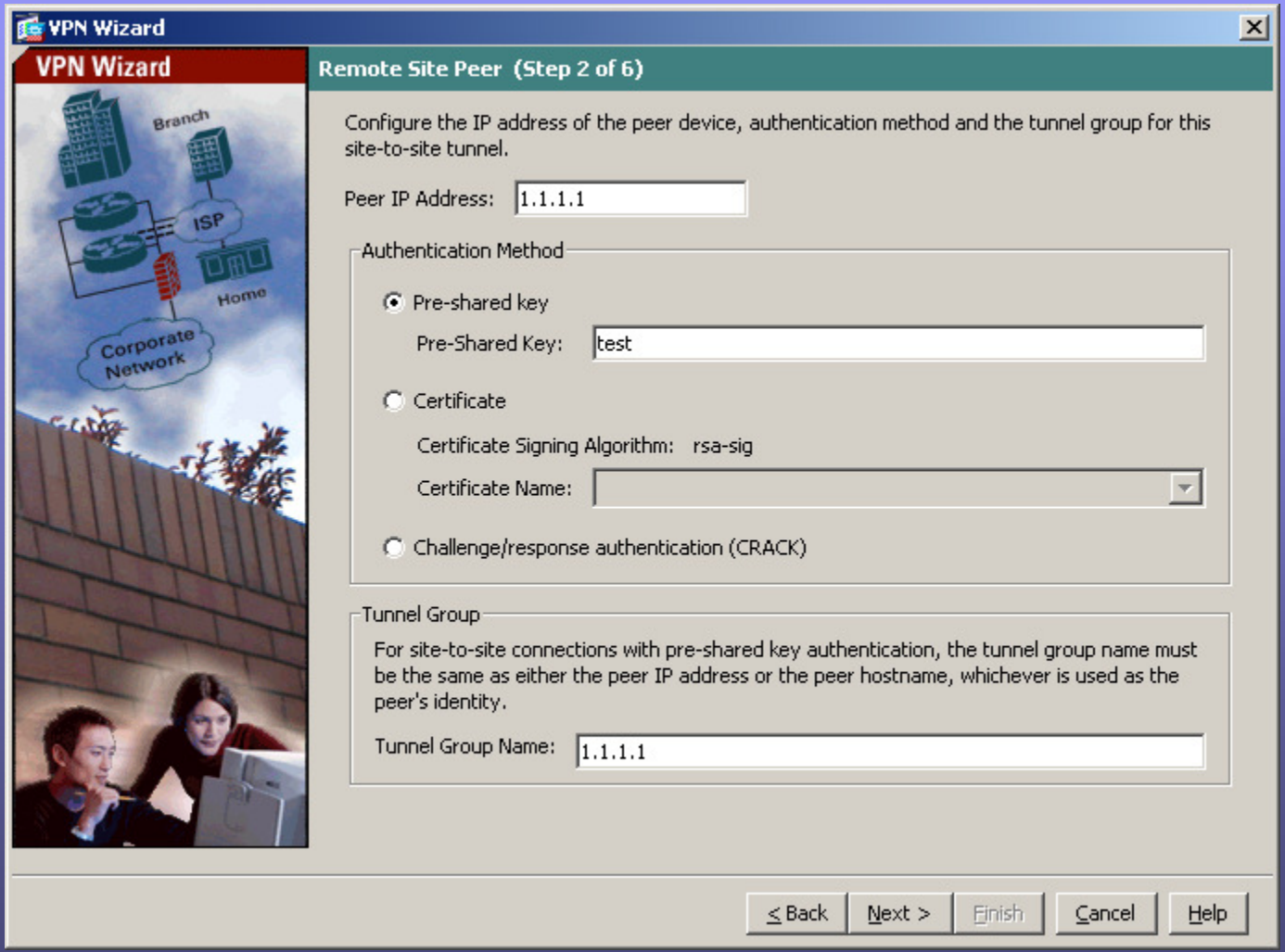
- When connected via telnet/ssh the command “terminal monitor” should be issued to see debug commands.
- To debug the IPSec connection, issue “Debug crypto isa”.
- To view the current SAs, issue the “show cry isa sa” command. When the tunnel is properly established, you should see :

```
Router#show cry isa sa

dst          src          state        conn-id slot status

1.1.1.2      1.1.1.1      QM_IDLE          4    0 ACTIVE
```

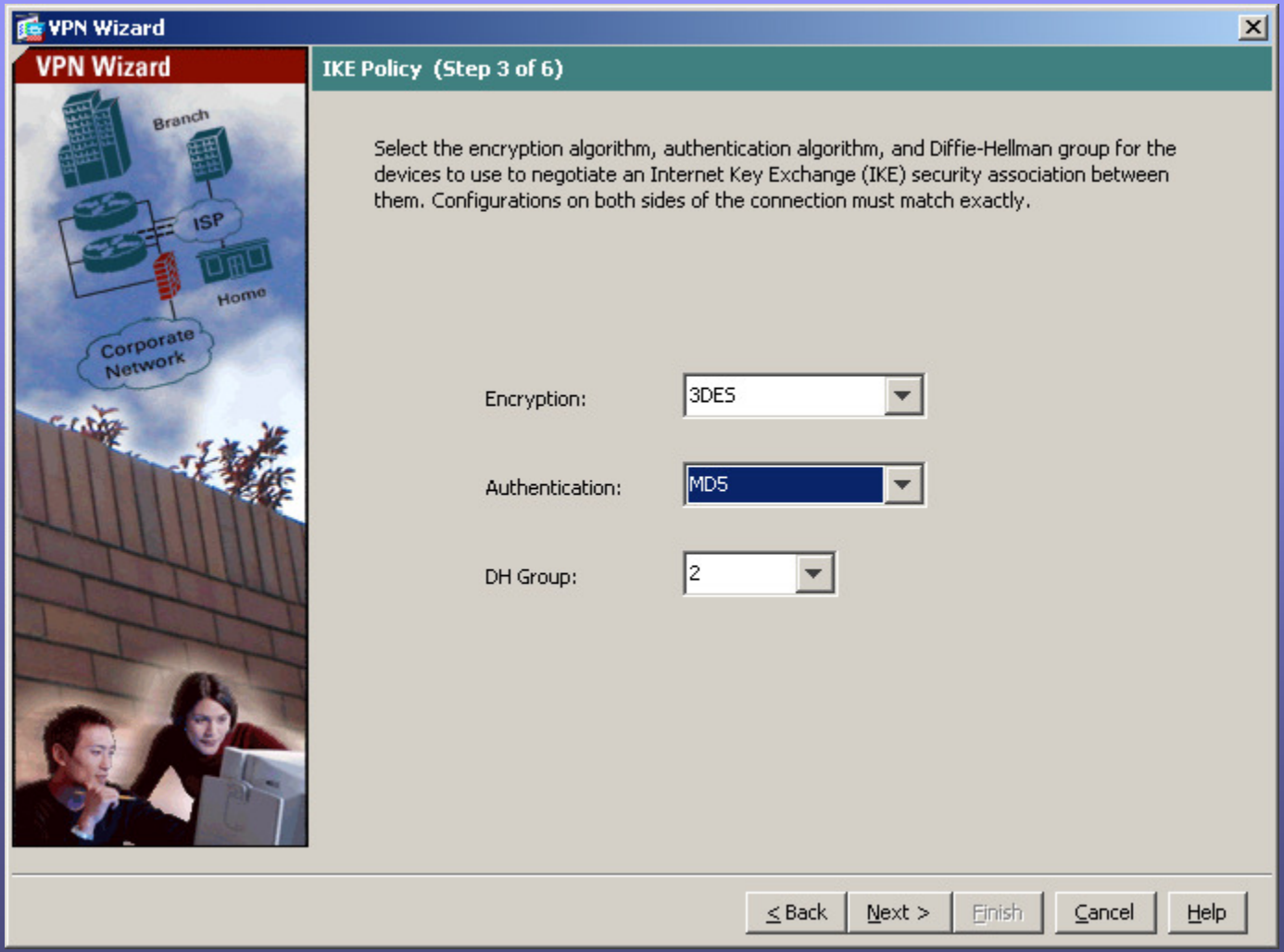
IPSec Tunnel – MTK to Cisco ASA - Site # 2



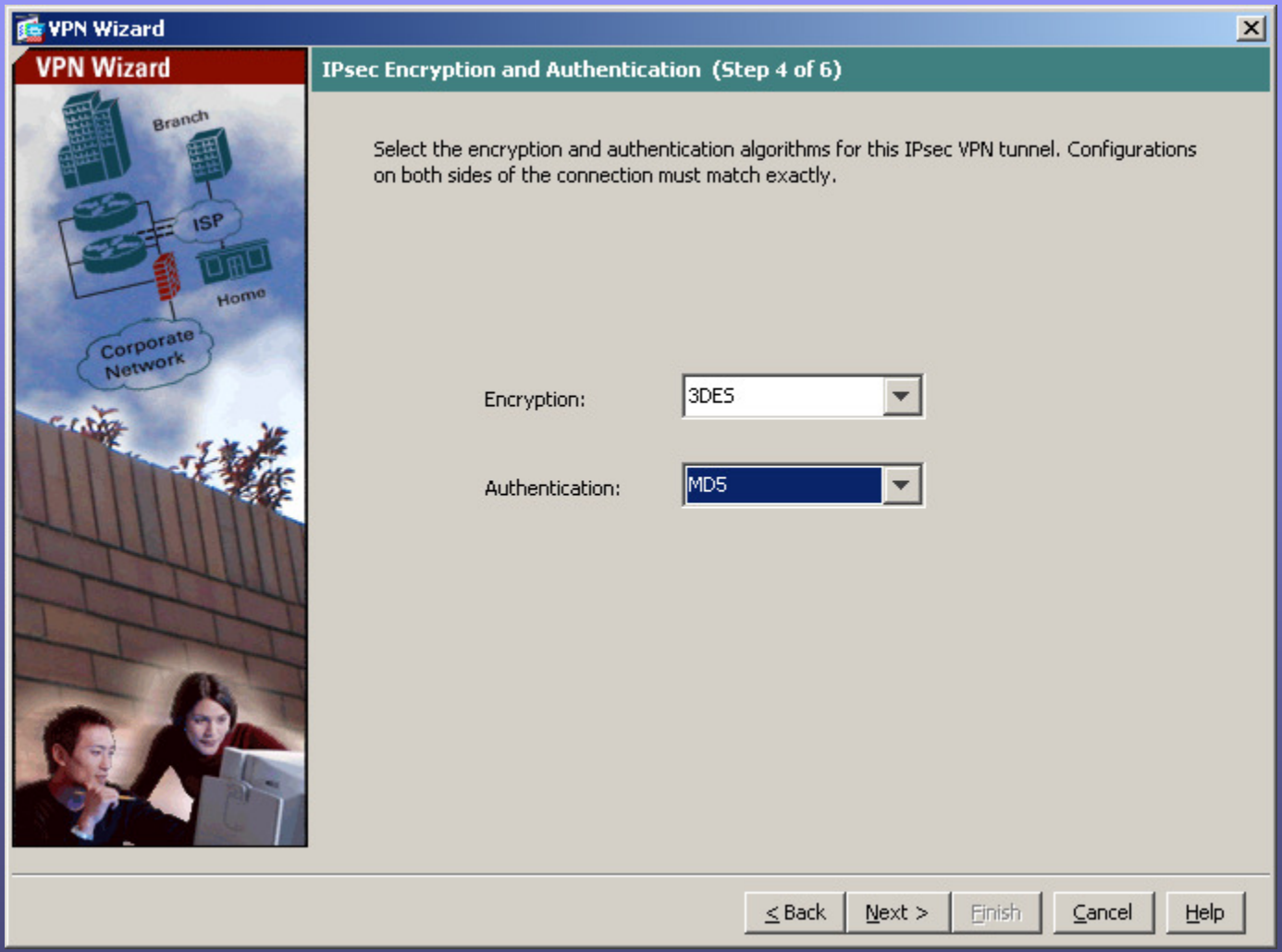
IPSec Tunnel – MTK to Cisco ASA - Site # 2



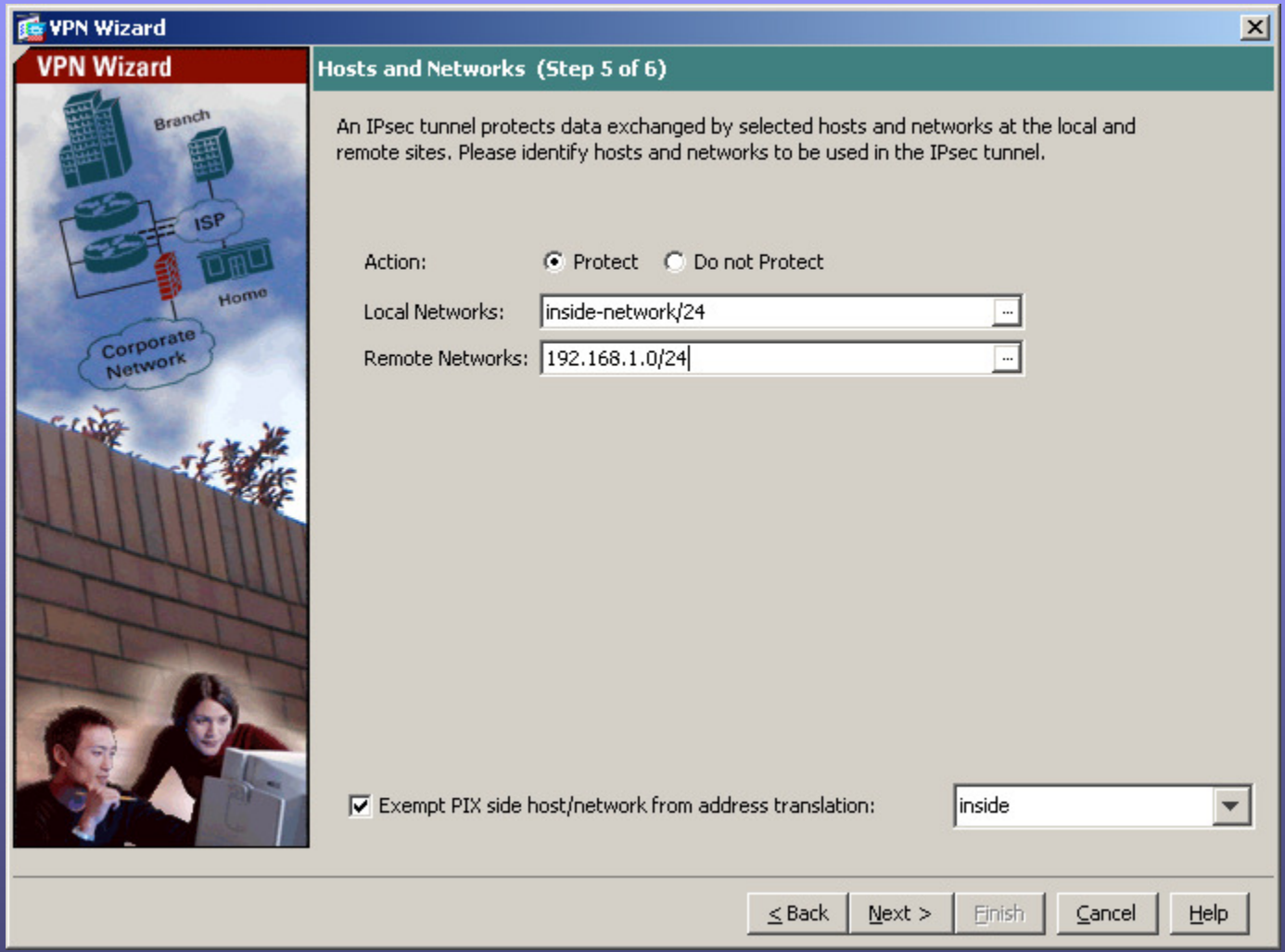
IPSec Tunnel – MTK to Cisco ASA - Site # 2



IPSec Tunnel – MTK to Cisco ASA - Site # 2



IPSec Tunnel – MTK to Cisco ASA - Site # 2



IPSec Tunnel – MTK to Cisco ASA - Site # 2

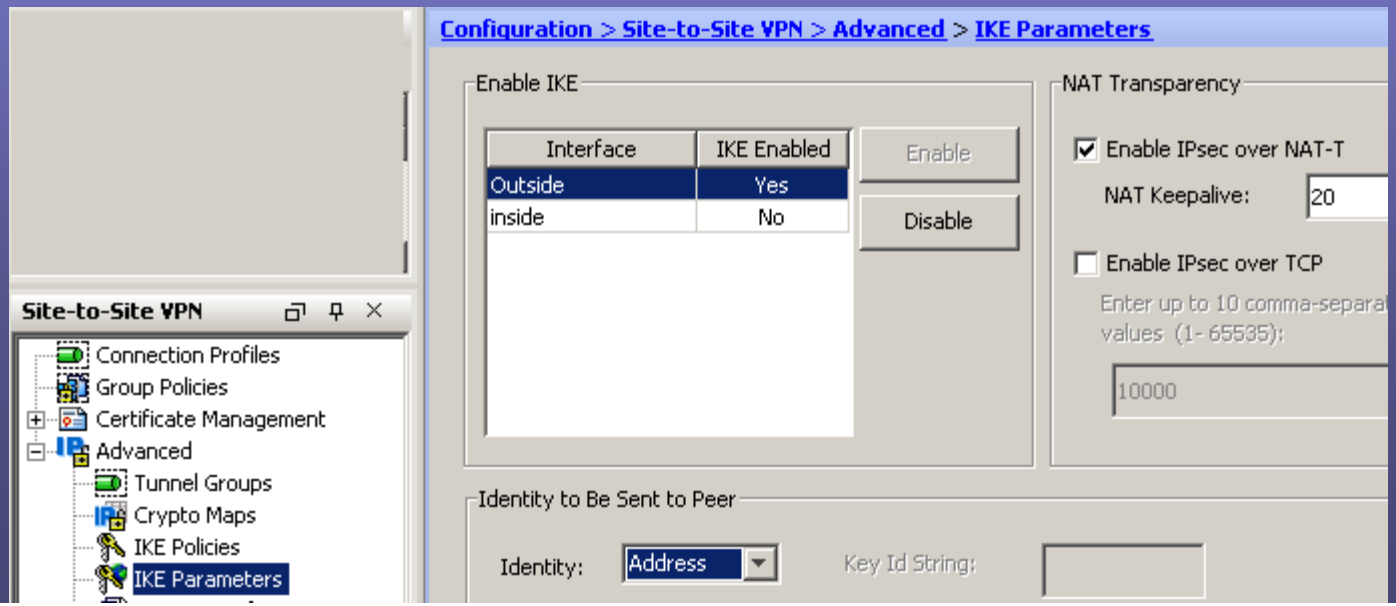
```
interface Ethernet0
 nameif Outside
 security-level 0
 ip address 1.1.1.2 255.255.255.252
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 192.168.2.1 255.255.255.0
!
access-list Outside_1_cryptomap extended permit ip 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
access-list inside_nat_outbound remark PAT all out
access-list inside_nat_outbound extended permit ip 192.168.2.0 255.255.255.0 any
access-list inside_nat0_outbound extended permit ip 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
!
global (Outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 access-list inside_nat_outbound
route Outside 0.0.0.0 0.0.0.0 1.1.1.1 1
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto map Outside_map 1 match address Outside_1_cryptomap
crypto map Outside_map 1 set pfs
crypto map Outside_map 1 set peer 1.1.1.1
crypto map Outside_map 1 set transform-set ESP-3DES-MD5
crypto map Outside_map 1 set security-association lifetime seconds 28800
crypto map Outside_map 1 set security-association lifetime kilobytes 4608000
crypto map Outside_map interface Outside
crypto isakmp enable Outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash md5
 group 2
 lifetime 86400
!
tunnel-group 1.1.1.1 type ipsec-l2l
tunnel-group 1.1.1.1 ipsec-attributes
 pre-shared-key test
```

IPSec Tunnel – MTK to Cisco ASA - Site # 2 Trouble shooting

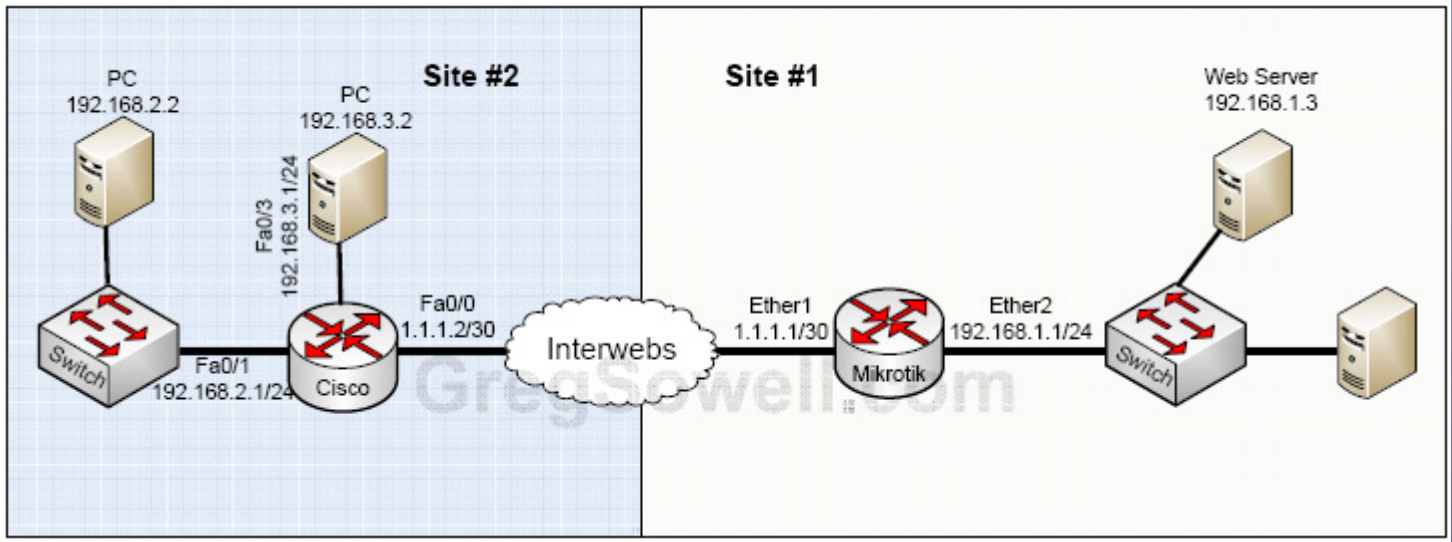
- You can issue the show “show cry isa sa” command and look for active.
- With debugging enabled, filter on the remote device’s IP.

IPSec Tunnel – MTK to Cisco ASA - Site # 2

- From the IKE parameters section. Change identity to be Address. I've found this to fix occasional IPSec connection issues.
- crypto isakmp identity address



IPSec Tunnel – MTK to Cisco RTR Multiple Subnets

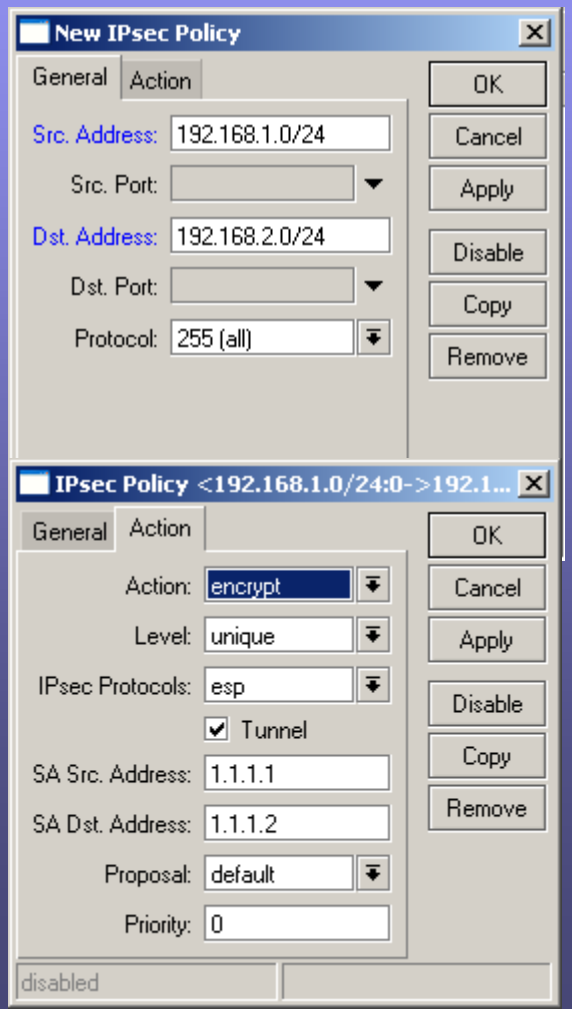


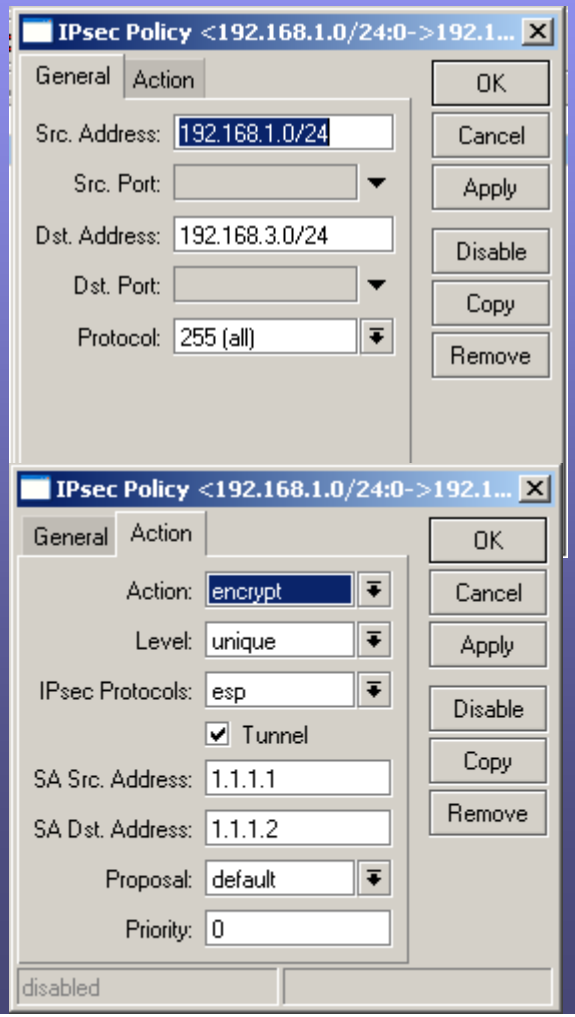
IPSec Tunnel – MTK to Cisco RTR - Site # 1

Create Peer/Proposal same as above

Create Policies

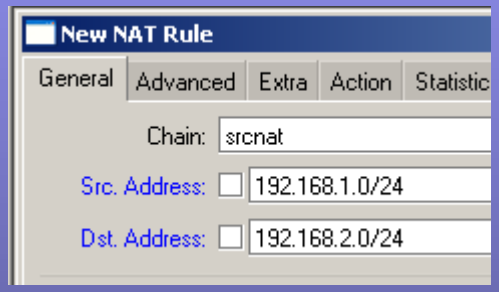
When connecting multiple subnets to a Cisco device, be it router or ASA, you will need to specify the level as unique. The Cisco device wants a separate SA for each policy coming back to it.



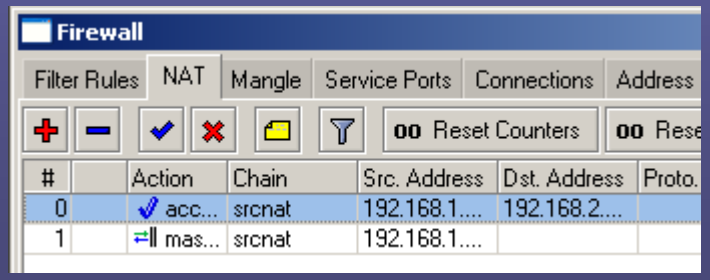


IPSec Tunnel – MTK to MTK - Site # 1

- IP -> Firewall -> NAT
- Create NAT bypass for traffic that should traverse the tunnel.



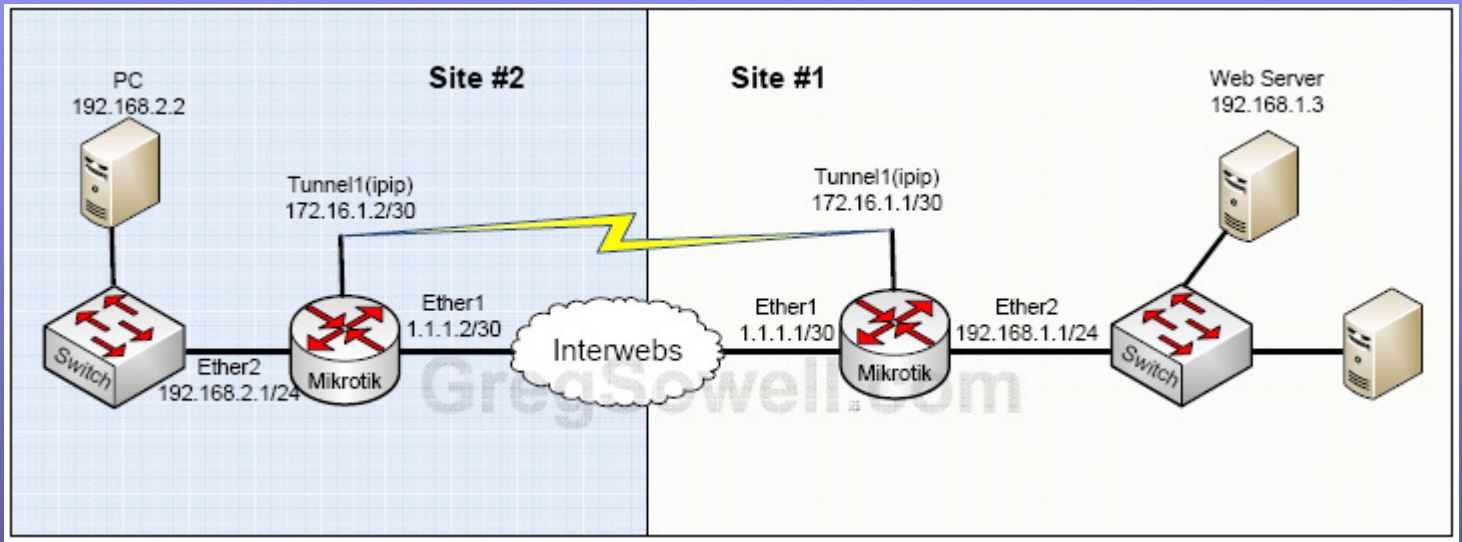
- Move the rule to the top.



IPSec Tunnel – MTK to Cisco RTR - Site # 2

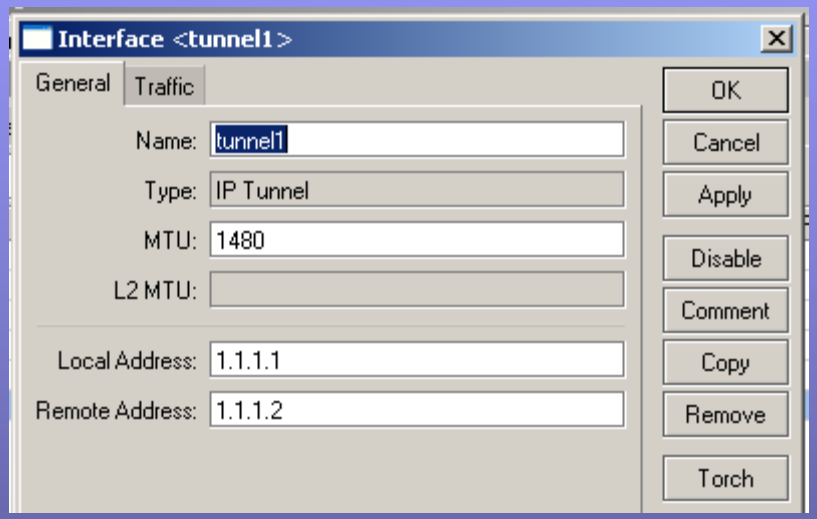
```
crypto isakmp policy 1
 hash md5
 encr 3des
 authentication pre-share
 group 2
 lifetime 14400

crypto isakmp key test address 1.1.1.1

crypto ipsec transform-set to_remotes esp-3des esp-md5-hmac

crypto map to_remotes 10 ipsec-isakmp
 set peer 1.1.1.1
 set transform-set to_remotes
 match address Kitchen

int e0
ip address 1.1.1.2 255.255.255.252
crypto map to_remotes
no shut

int e1
ip address 192.168.2.1 255.255.255.0
no shut

int e2
ip address 192.168.3.1 255.255.255.0
no shut

ip route 0.0.0.0 0.0.0.0 1.1.1.1

ip nat inside source list NAT interface e0 overload

ip access-list extended Kitchen
 remark Allow access though tunnel to Kitchen LAN
 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255


ip access-list extended NAT
 deny   ip any 192.168.0.0 0.0.255.255
 permit ip any any
```

IPSec Tunnel – MTK to MTK
IPIP tunnel w/ IPSec

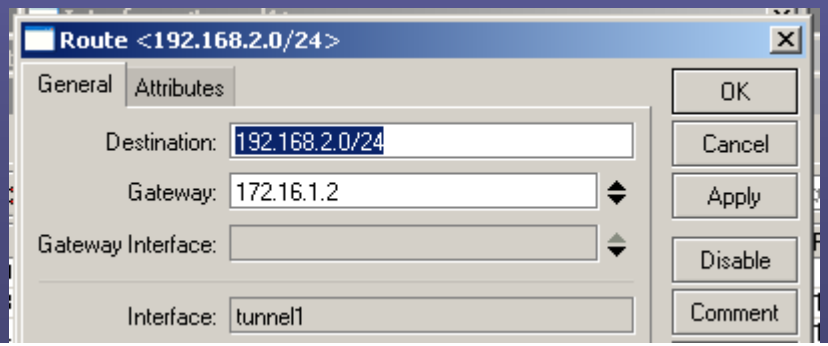


IPSec Tunnel – MTK to MTK IPIP - Site # 1

- Create Tunnel Interface

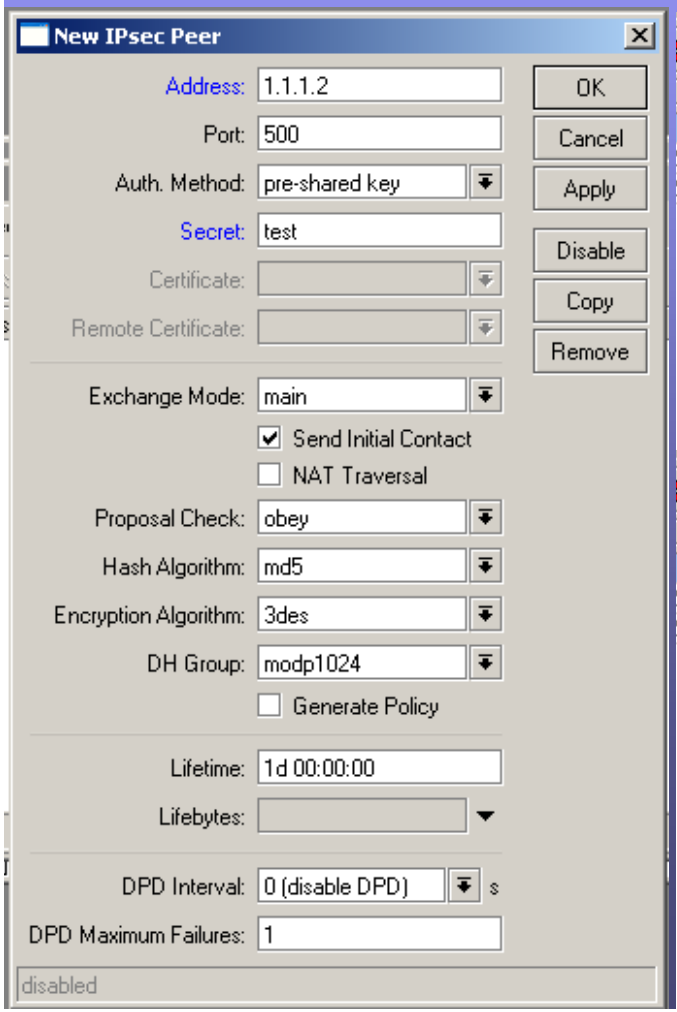


- Create routes to other location to head through Tunnel

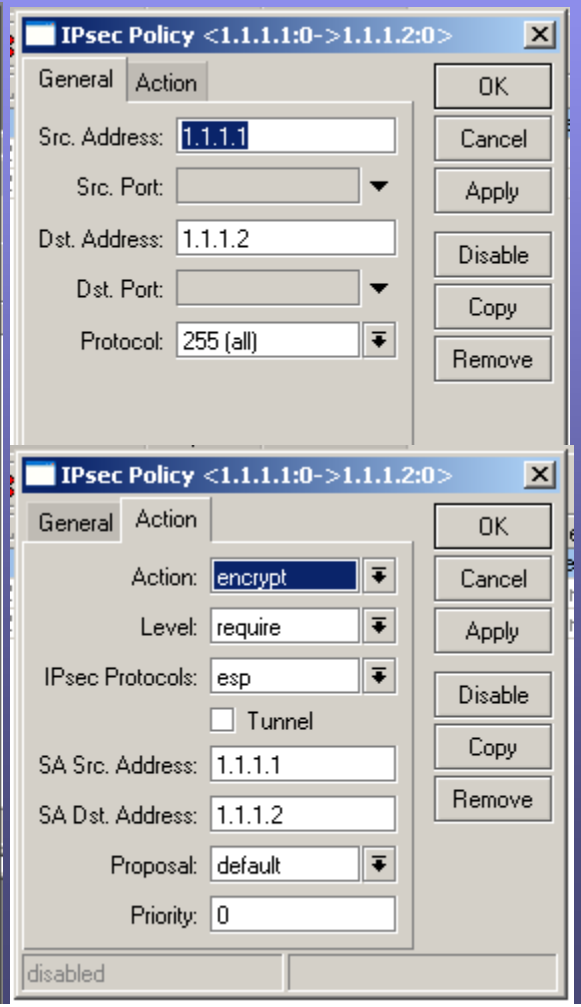


IPSec Tunnel – MTK to MTK IPIP - Site # 1

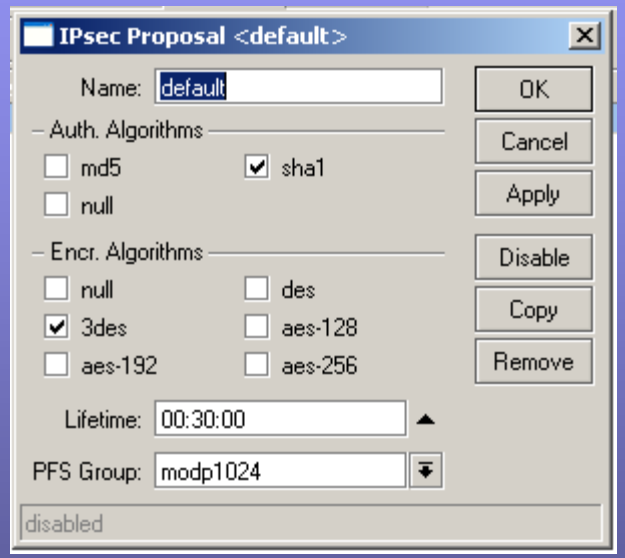
Create Peer



Create Policy



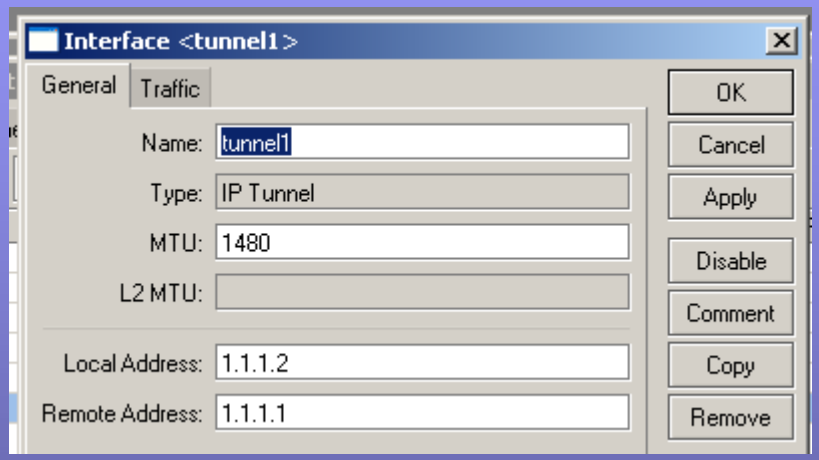
Create/Modify proposal if you



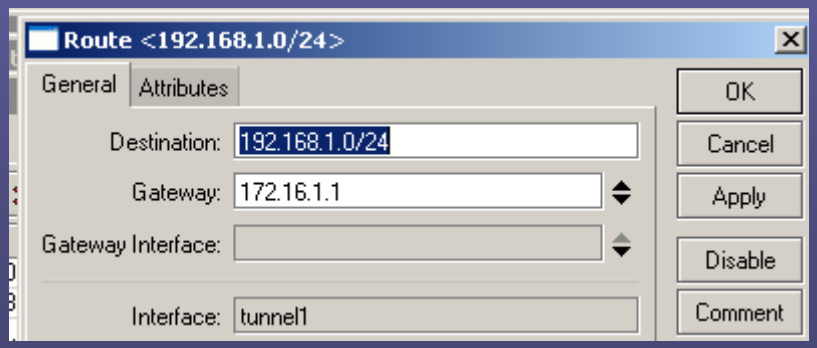
Note we are using transport mode, so the tunnel check box isn't ticked.

IPSec Tunnel – MTK to MTK IPIP - Site # 2

- Create Tunnel Interface

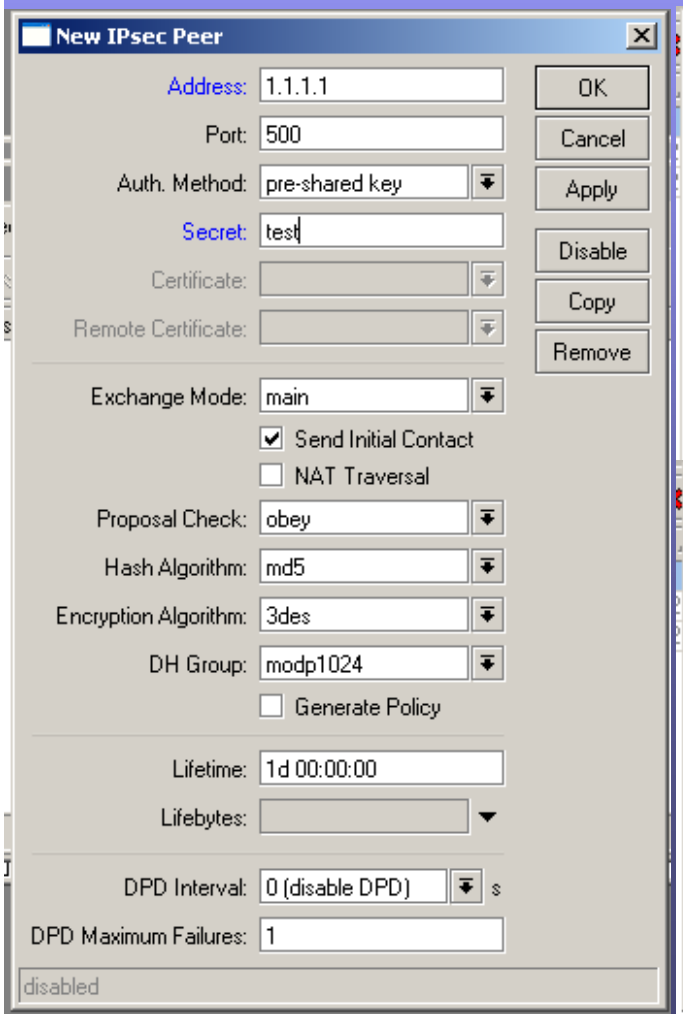


- Create routes to other location to head through Tunnel

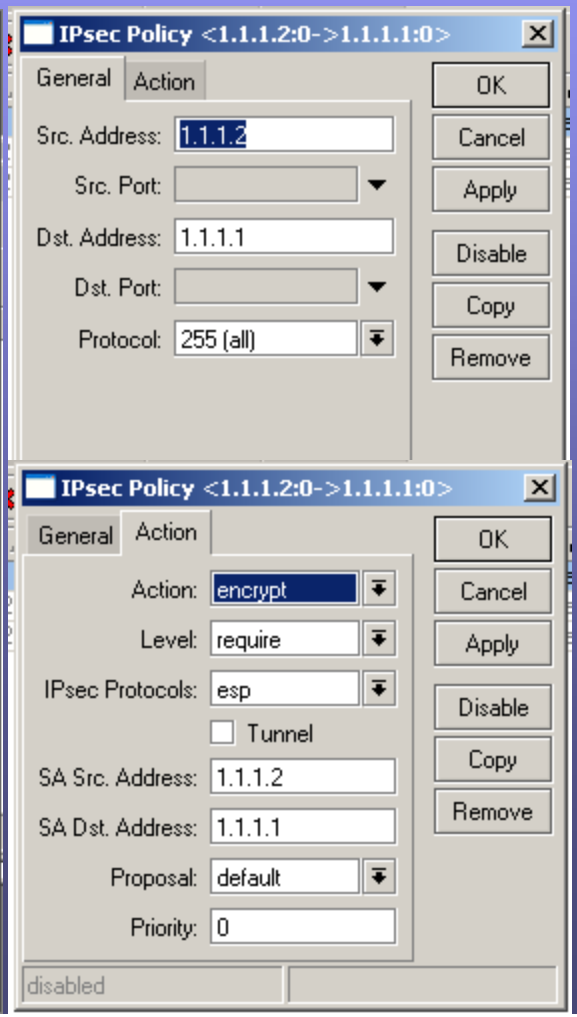


IPSec Tunnel – MTK to MTK IPIP - Site # 1

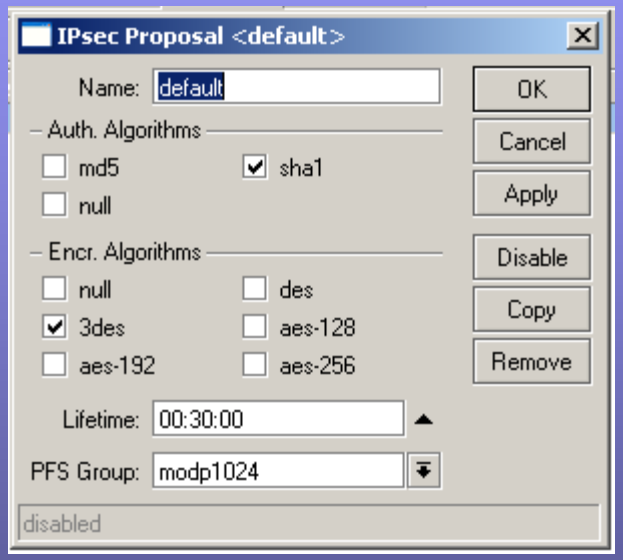
Create Peer



Create Policy

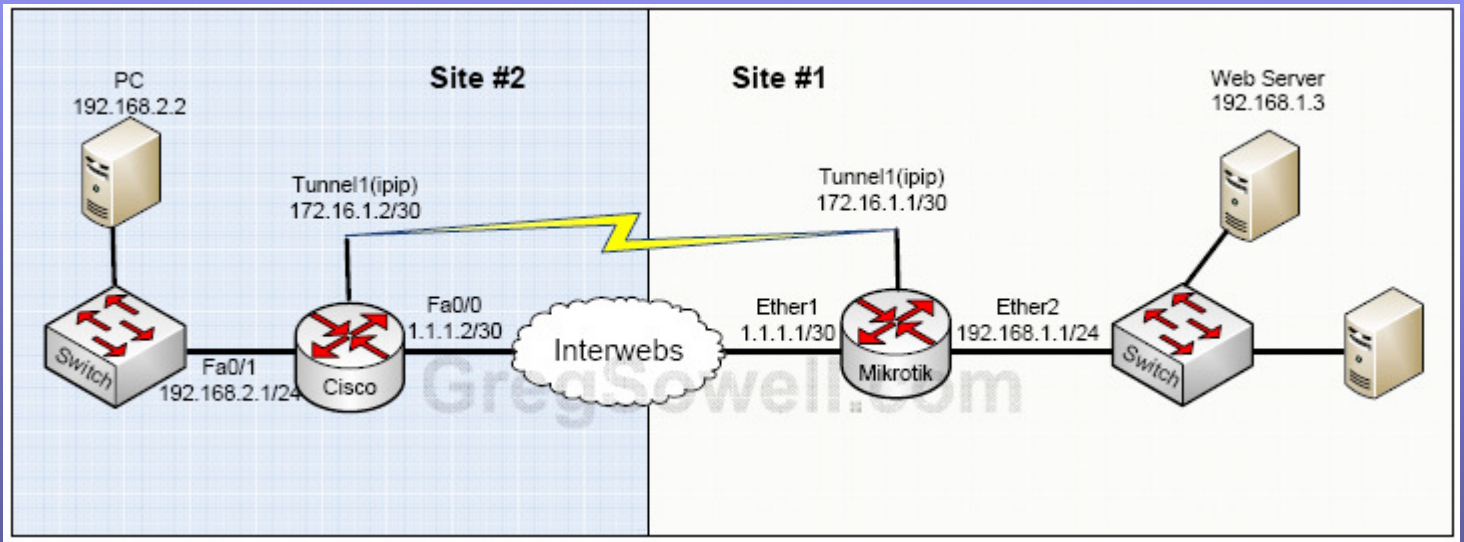


Create/Modify proposal if you



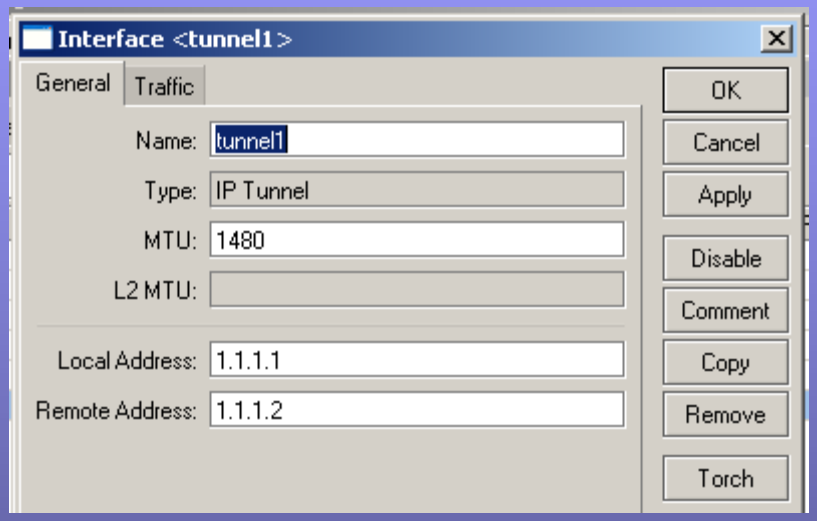
Note we are using transport mode, so the tunnel check box isn't ticked.

IPSec Tunnel – MTK to Cisco Rtr IPIP tunnel w/ IPSec

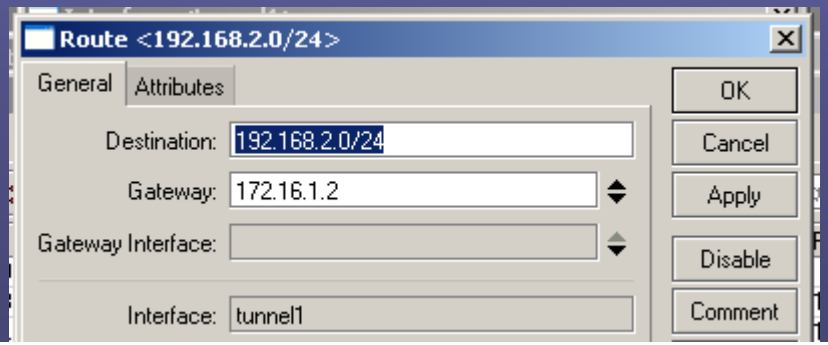


IPSec Tunnel – MTK to Cisco IPIP - Site # 1

- Create Tunnel Interface

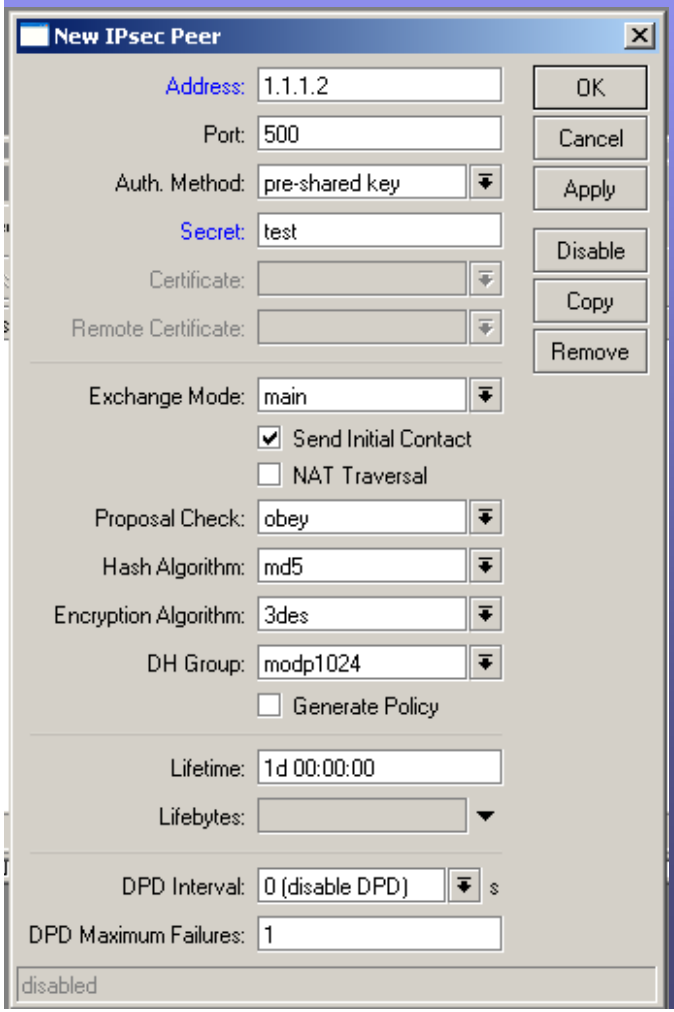


- Create routes to other location to head through Tunnel

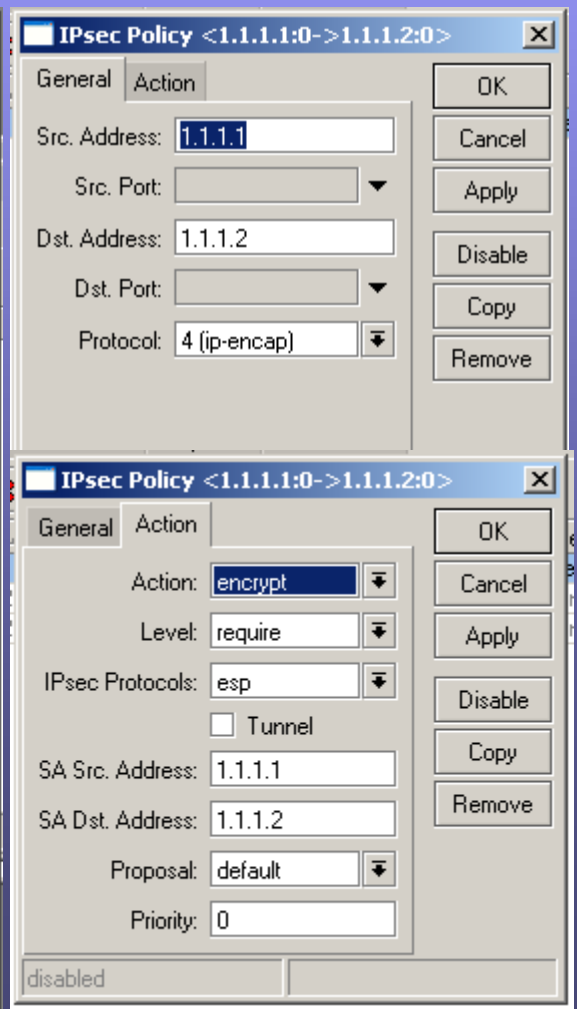


IPSec Tunnel – MTK to Cisco IPIP - Site # 1

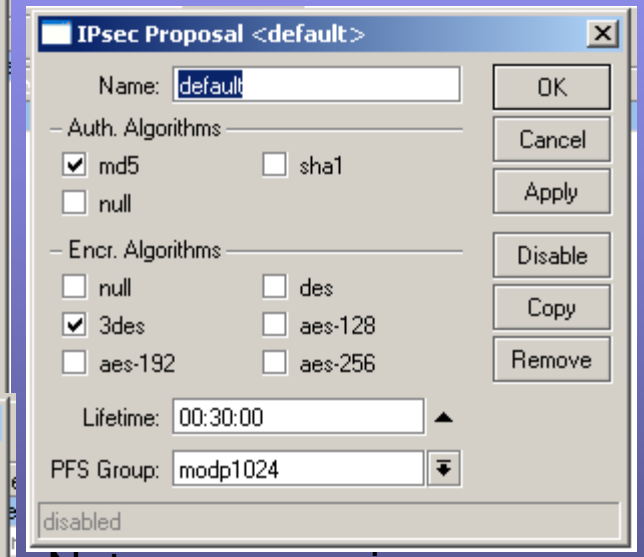
Create Peer



Create Policy



Create/Modify proposal if you choose



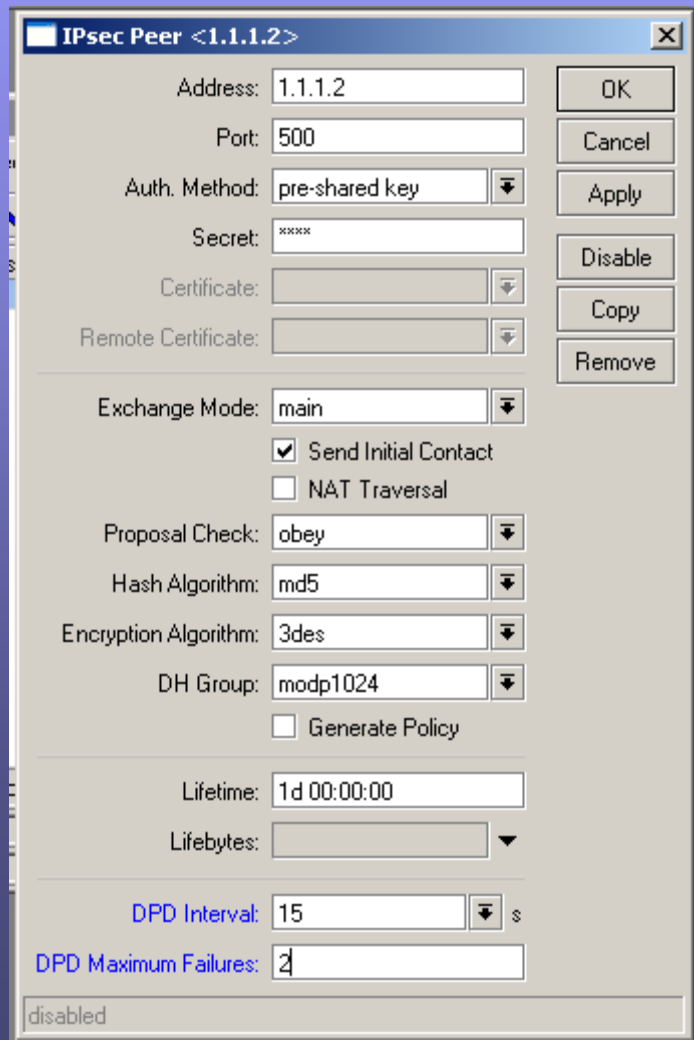
Note we are using transport mode, so the tunnel check box isn't ticked. Also note we set the protocol to 4 IP-Encap. This catches only IPIP traffic.

IPSec Tunnel – MTK to Cisco IPIP - Site # 2

```
crypto isakmp policy 1
 hash md5
 encr 3des
 authentication pre-share
 group 2
 lifetime 14400

crypto isakmp key test address 1.1.1.1

crypto ipsec transform-set to_remotes esp-3des esp-md5-hmac
mode transport

crypto map to_remotes 10 ipsec-isakmp
 set pfs group2
 set peer 1.1.1.1
 set transform-set to_remotes
 match address IPIP

int e0
ip address 1.1.1.2 255.255.255.252
crypto map to_remotes
no shut

int ep1
ip address 192.168.2.1 255.255.255.0
no shut

ip route 0.0.0.0 0.0.0.0 1.1.1.1
ip route 192.168.1.0 255.255.255.0 172.16.1.1

ip nat inside source list NAT interface e0 overload

ip access-list extended IPIP
 remark Allow IPIP traffic
 permit ipinip host 1.1.1.2 host 1.1.1.1

ip access-list extended NAT
 deny   ip any 192.168.0.0 0.0.255.255
 permit ip any any
```

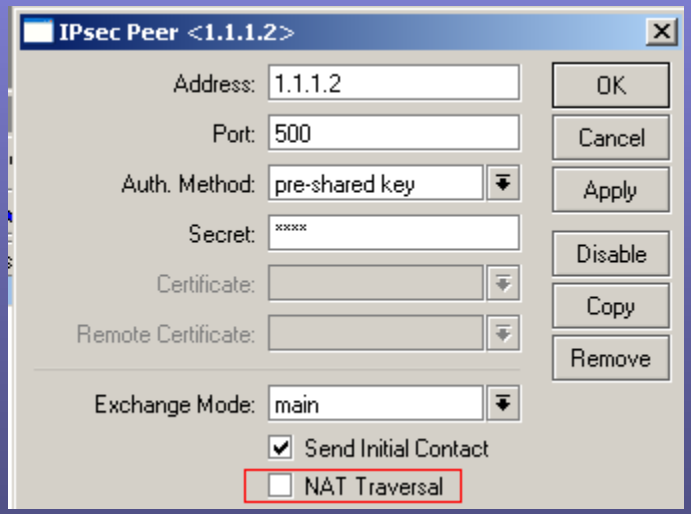
IPSec Dead Peer Detection(DPD)

- DPD is an extremely useful tool when connecting to Cisco equipment.
- The DPD interval is number of seconds that the remote side is unresponsive.
- Once the DPD interval has met the Max Failures, it will clear out the SAs to this host and attempt to establish a new SA.



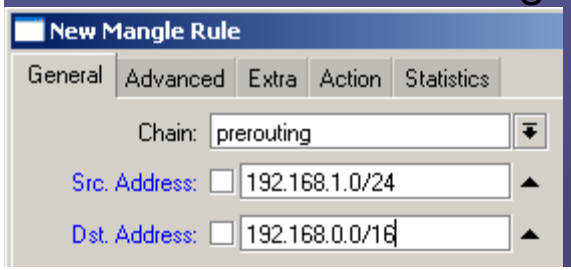
NAT Traversal

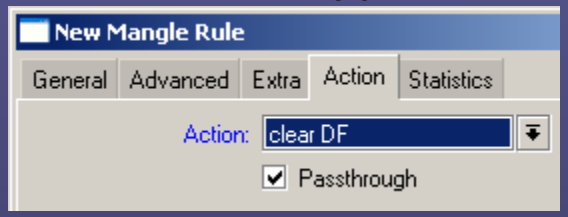
- NAT traversal in Mikrotik should NEVER be used unless absolutely necessary.



Clear DF

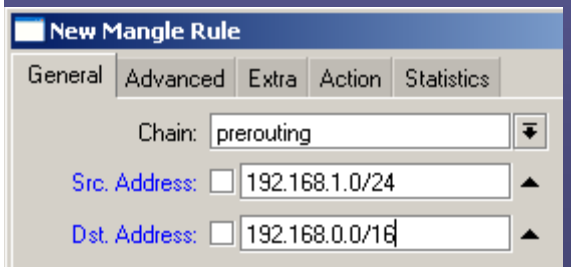
- The DF(Do not Fragment) bit can be set in packets at the sending device.
  - Microsoft exchange communication sets DF
  - Microsoft terminal services sets DF
- The DF bit tells a router that if the MTU of the packet is too large to traverse, do not fragment the packet, just drop. Generally a router will then send back a special ICMP message telling the router to readjust the MTU. When a packet tries to go through an IPSec tunnel and is dropped do to MTU issues, no message is generated because an IPSec tunnel isn't a physical or virtual interface. This means the traffic is simply lost.
- If you clear the DF bit on traffic that is set with the DF bit, it will then be allowed to fragment on the router and will successfully pass through the tunnel.
- A good indicator of DF issues with MTU would be attempting to RDP to a windows machine across a tunnel. Your screen will go black or blue, but the login box will never appear.
- The below mangle rule would be applied at site 1 in our demonstrations.

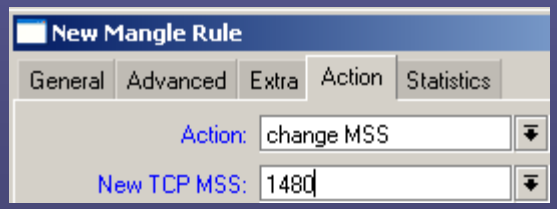




Change MSS

- If you are having MTU issues going through an IPSec tunnel, you can adjust the MTU on the inside interface, thus affecting all traffic, VPN and not, or one can alternately change the MSS (Maximum Segment Size) of the TCP traffic passing through an IPSec tunnel.
- This is also accomplished via a mangle rule.





Diffie Hellman Group Map

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

From the wiki http://wiki.mikrotik.com/wiki/IPsec#Diffie-Hellman_Groups

Resources

- Awesome Site – http://GregSowell.com
- Mikrotik Video Tutorials - http://gregsowell.com/?page_id=304
- Mikrotik Support Docs- http://www.mikrotik.com/testdocs/ros/3.0/
- CactiEZ - http://cactiez.cactiusers.org/download/
- Cacti Video Tutorials - http://gregsowell.com/?page_id=86
- Great Consultant ;)- http://gregsowell.com/?page_id=245