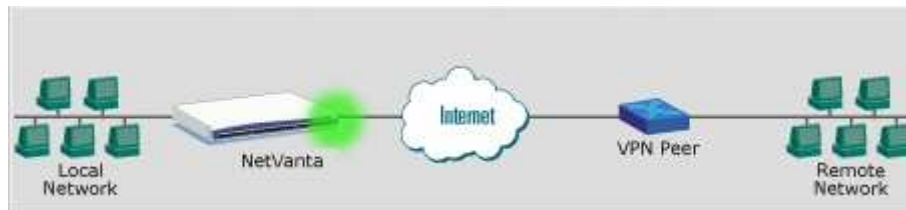


Configuring a VPN using Main Mode in AOS

This guide explains how to configure a VPN Tunnel between an Adtran OS (AOS) device and any other IPSEC VPN compliant device that supports Main Mode. If you are attempting to create a VPN tunnel with a device that does not have a static IP address, you should consult the guide titled “Configuring a VPN using Aggressive Mode in AOS”.



Information Requirements

You will need all of the following information to be able to establish a VPN using Main Mode. If the VPN peer is not an AOS device, you will need some additional information:

- Public IP of Both VPN devices
 - These must be static, or never changing IPs
- Network IP Addresses and Subnet Masks for both private networks
 - Example: 192.168.1.0 /24 and 10.10.10.0 /24

For Peers that are not an AOS device:

- Supported IKE Encryption Algorithms
- Supported IKE Hash Algorithms
- Supported Diffie-Helman Group
- Supported IPsec Encryption Algorithms
- Supported IPsec Hash Algorithms

Hardware Requirements

To implement an IPsec VPN using Main Mode in AOS you will need the following items.

- An Adtran OS Router
 - Example: Netvanta or Total Access
- Enhanced Feature Pack for each Adtran OS Device
- Power Cable for AOS Device

Software Requirements

Before implementing a VPN, you should already have connectivity established between the two devices. An acceptable test is the ability to ping the Public IP Address of one VPN Peer from the console of the other peer.

Configuring

This guide includes instructions for both the Web Interface and the Command Line Interface. You should use only one method, not both. For users unfamiliar with the Command Line Interface (Console Port and Telnet), the Web Interface is highly recommended. The Web Interface also includes a “VPN Wizard” that provides step-by-step configuration of a VPN. The “VPN Wizard” equivalent for this guide is a “Typical Setup” using a “Static Peer”.

Example Settings

The following information will be used as example settings for this guide. You should not copy these settings verbatim. You should evaluate this example guide and apply your own settings as needed. Excluding IP addresses, these example settings will always work when connecting two Adtran OS VPN devices. You will need to research supported attribute types for other VPN vendor’s equipment.

Setting	Router A*	Router B
Local ID (Type)	5.5.5.5 (IP Address)	6.6.6.6 (IP Address)
Remote ID (Type)	6.6.6.6 (IP Address)	5.5.5.5 (IP Address)
Pre-Shared Key	0123456789	0123456789
IKE Hash Algorithm	SHA-1	SHA-1
IKE Encryption Algorithm	3DES	3DES
Diffie-Helman Group	1	1
IPSec Hash Algorithm	SHA-1	SHA-1
IPSec Encryption Algorithm	3DES	3DES
Local Private Network	192.168.1.0 /24	10.10.10.0 /24
Remote Private Network	10.10.10.0 /24	192.168.1.0 /24

* Only the steps for configuring Router A are shown in this guide

Configuring you via the Web Interface

Login to the Web Interface of your AOS device. If you do not have access to the Web Interface of your AOS device, consult the guide “Enabling the Web GUI in AOS”.

Click ‘VPN Peers’ in the left menu. If you do not see a VPN section in the left menu, your AOS device does not have the Enhanced Feature Pack. The Enhanced Feature Pack includes all of the software required for creating a VPN connection.

Check the **Enable** checkbox.



VPN Enabled:

Apply

Click **Apply**.

Choose **<Default>** from the drop down box, and click **Create New VPN Peer**.

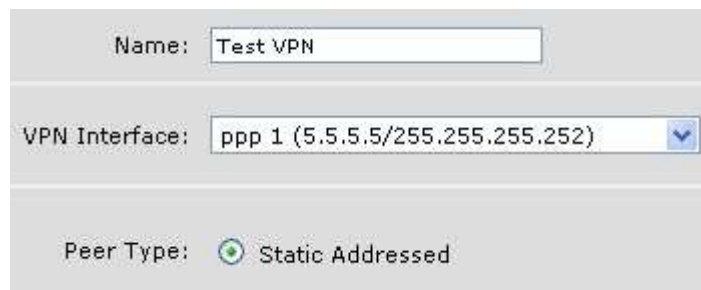


Create a New VPN Peer based on the <Default> Peer

Create New VPN Peer

Enter a **Name** for the VPN Peer; Example 'Test VPN'.

Select the **VPN Interface** from the drop down box. The VPN Interface is the Public IP interface on this AOS Device; the interface that has is assigned a Public IP. In this example, the AOS Device uses a PPP connection over a T1 for Internet Access.



Name: Test VPN

VPN Interface: ppp 1 (5.5.5.5/255.255.255.252)

Peer Type: Static Addressed

Select **Static Addressed** for the Peer Type. If the peer does not have a static IP address, you should use the guide titled "VPN using Aggressive Mode" instead of this guide.

Click **Apply**.

IKE (Phase 1) Settings, part 1:

Scroll down to 'IKE Configuration'. The following settings apply to the IKE portion or Phase 1 one the VPN negotiation.

Choose **Main** for 'Initiate Mode'. This AOS device will attempt to negotiate using Main Mode in Phase 1.



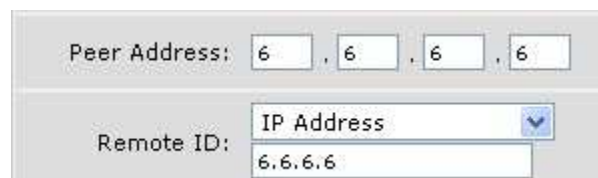
Initiate Mode: Main

Respond Mode: Any

Choose **Any** for 'Respond Mode'. This AOS device will respond to both Main and Aggressive Mode for Phase 1.

Choose **Allow V1** and **Allow V2** for 'NAT Traversal'. If this VPN will be connecting to a non-AOS device, and you find that after properly configuring the VPN on both peers the VPN does not work, choose disable for both NAT Traversal versions.

Enter the **Peer Address**; this example uses 6.6.6.6



Peer Address: 6 . 6 . 6 . 6

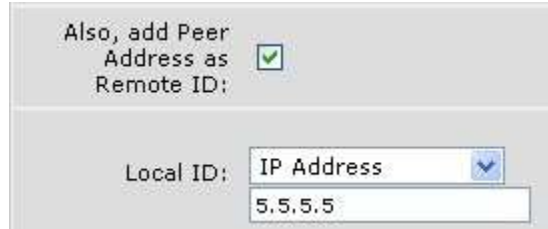
Remote ID: IP Address
6.6.6.6

Choose **'IP Address'** for the Remote ID Type and enter the VPN peer's IP address; this example uses 6.6.6.6

Enter a **Pre-Shared Key**; this example uses '0123456789'. The pre-shared key can be any string of characters you like and must be the same on both VPN peers.

Check **'Also add Peer Address as Remote ID'**. This will automatically add the appropriate Remote ID.

Choose **'IP Address'** for the Local ID Type. Enter this AOS devices' public IP.



Also, add Peer Address as Remote ID:

Local ID:

IPSec (Phase 2) Settings:

The following settings apply to the IPSec or Phase 2 portion of the VPN negotiation.

Choose **'Group 1'** for PFS.

Choose **'ESP: 3 DES / SHA1'** for the Encryption / Hash Algorithm. This sets Triple-DES (3DES) and SHA-1 as the encryption and Hash Algorithm for Phase 2.

Enter **'28800'** for Lifetime Seconds and leave Lifetime KB blank.



IPSec Configuration

PFS:

Encryption / Hash:

Encryption / Hash:

Lifetime: seconds
 KB

Click **'Apply'**.

IKE (Phase 1) Settings, part 2:

The following settings apply to the IKE or Phase 1 portion of the VPN Negotiation.

Scroll down to "Step 2 ..."

Choose **'3 DES'** and **'SHA1'** for the 'Encryption / Hash' settings.

Choose **'Preshared Key'** for Authentication.



Encryption / Hash: /

Authentication:

DH Group:

Lifetime: seconds

Select **'1'** for DH Group; this is the Diffie-Helman Group setting.

Enter **'28800'** seconds for the Lifetime.

Click **'Add'**.

Negotiated Network Settings:

Scroll down to "Step 3..."

IPSec negotiation includes negotiating which networks will be allowed to communicate across the VPN. Step 3 identifies these source and destination networks.

Click **'Add New VPN Selectors'**.

Choose **'Permit'** for the 'Filter Type'.

Filter Type: Permit
 Deny

Protocol: any [v] []

Choose **'Any'** for the 'Protocol'.

Select **'IP Address'** for the 'Source Host/Network'.

Any
 IP Address

Address: 192 . 168 . 1 . 0
Mask: 255 . 255 . 255 . 0

Enter the Network IP Address of the local private network and the appropriate Subnet Mask. This example uses 192.168.1.0 with a 255.255.255.0 Subnet Mask.

Select **'IP Address'** for the 'Destination Host/Network'.

Any
 IP Address

Address: 10 . 10 . 10 . 0
Mask: 255 . 255 . 255 . 0

Enter the Network IP Address of the remote private network and the appropriate Subnet Mask. This example uses 10.10.10.0 with a 255.255.255.0 Subnet Mask.

Click **'Apply'**.

Scroll back down to "Step 3..."

Delete the 'deny any any' rule in the 'Modify/Delete VPN Selector Entry' list.

Dest Network/Ports	
any	Delete
10.10.10.0/24	Delete

Configuration for the Firewall:

If the firewall of your AOS device is enabled, you will need to allow the VPN tunnels through the firewall. This is accomplished by scrolling to the bottom of the VPN Peer page, and checking the checkboxes for all Security Zones.

Click **Apply** when finished.

Saving the Configuration:

It is important that you save your configuration!

After you have completed configuring your AOS router, click the ‘**Save**’ button in the top right corner.

You should also consider downloading the configuration to your desktop. This ensures that you will always have a backup copy of the configuration for your router.

Click ‘**Configuration**’ in the left hand menu.

Click ‘**Download Configuration**’. Save this file on your computer, and create backup copies. You can use this file to restore your router to its current settings.



Figure 1 - Save Button



Figure 2 - Download Button

Configuring via the Command Line Interface

VPN using Main Mode can be completely configured via the command line interface. Those users unfamiliar with the Command Line Interface are advised to use the Web Interface for configuration. To learn how to enable the Web Interface, consult the guide titled “Enabling the Web GUI”.

The Command Line Interface uses several groups of information to create a single VPN. The following is a list of groups of information you will create to configure a VPN.

- IKE Policy
- IPsec Policy
- Remote ID Entry
- IPsec Transform Set
- VPN Selector Access Lists

Gaining Access to Configuration Mode:

Type the command **enable** to access Enable Mode. If you do not know the enable password, consult the document titled “I lost the password to my AOS device”.

Type the command **configure terminal** to enter Global Configuration Mode.

Type **ip crypto** to enable the VPN engine in the AOS device.

Configuring the IKE Policy:

The following configuration defines the IKE or Phase 1 attributes used to negotiate this VPN. This IKE policy will be referenced in the IPSec Policy and the Remote ID Entry.

Type **crypto ike policy 100** to create an IKE policy for the VPN. The number ‘10’ in this example is imply a unique identifier for this policy. You may choose any number you like, but it must be unique in this AOS device.

Type **initiate main** to configure this as a VPN negotiated using Main Mode.

Type **respond anymode** to allow this IKE policy to negotiate both Main and Aggressive Modes.

Type **local-id address 5.5.5.5**. This example uses 5.5.5.5 as this AOS device’s public ip address, but you should substitute your own address.

Type **peer 6.6.6.6**. This example uses 6.6.6.6 as peer’s public ip address, but you should substitute your own peer’s address.

Type **attribute 1** to create the first attribute set for IKE.

Type **hash sha** to set SHA-1 as the proposed Hash Algorithm for IKE.

Type **encryption 3des** to set 3DES as the proposed Encryption Algorithm for IKE.

Type **lifetime 28800** to set the lifetime of the IKE security association 28800 seconds.

Type **group 1** to set the Perfect Forward Secrecy (PFS) group to Diffie-Helman group 1.

Type **exit** to leave attribute settings.

Type **exit** again to leave the IKE Policy settings.

Creating the IPSec Transform Set:

The IPSec Transform Set creates a set of Encryption and Hash Algorithms to be used in the IPSec negotiation. This IPSec Transform Set will be referenced in the IPSec Policy.

Type **crypto ipsec transform-set HIGHLY-SECURE esp-3des esp-sha-hmac** to create a transform set named “HIGHLY-SECURE” that uses 3DES and SHA as encryption and hash algorithms.

Type **mode tunnel** to set the VPN to Tunnel mode.

Type **exit** to leave the transform-set configuration.

Configuring the IPSec Policy:

The following configuration establishes the IPSec policy and ties it with the IKE policy created above. The IPSec policy will reference the transform set created in the previous section and the VPN Selectors access list created later in this guide. This IPSec policy will also be referenced in the public IP interface configuration shown later in this guide.

Type **crypto map VPN 10 ipsec-ike** to create an IPSec policy named ‘VPN’ with a relative priority of 10. Additional IPSec policies named ‘VPN’ with higher or lower matching priorities.

Type **ike-policy 100** to link this IPSec policy with the IKE policy created above.

Type **set pfs group1** to enable Perfect Forward Secrecy and use Diffie-Helman Group 1.

Type **set security-association lifetime seconds 28800** to configure an IPSec Security Association lifetime of 28,800 seconds.

Type **set transform-set HIGHLY-SECURE** to link this IPSec policy with the IPSec transform set created in the previous section.

Type **match address VPN-10-SELECTORS** to reference the access-list that defines the VPN network addresses. This access-list will be created later in this guide.

Type **exit** to leave the IPSec configuration mode.

Configuring the Remote ID:

The Remote ID identifies the VPN peer and matches that peer’s Local ID setting. The Remote ID configuration references the IKE and IPSec policy, defines the pre-shared key and set several connection options.

Type **crypto ike remote-id address 6.6.6.6 preshared-key 0123456789 ike-policy 100 crypto map VPN 10 no-xauth no-mode-config** to create the Remote ID for the VPN Peer. This example uses 6.6.6.6 as the VPN Peer’s public address, but you should substitute your own peer’s public address. This example uses ‘0123456789’ as the preshared key.

Configuring the VPN Selector Access-List:

The following configuration creates an extended access-list that identifies the traffic to be transported across the VPN and defines the networks allowed to communicate across the VPN. This access-list is referenced in the IPSec Policy. If the ip firewall in AOS is enabled, it is imperative that this access-list be added as an allow statement to the appropriate policy-classes; this will be shown later in this guide.

Type **ip access-list extended VPN-10-Selectors** to create the access-list.

In this example the local private network is 10.10.10.0 /24 and the remote private network is 192.168.1.0 /24. The following line identifies the local and remote private networks that are allowed to communicate across this VPN. You will need to substitute your own private networks.

Type **permit ip 10.10.10.0 0.0.0.255 192.168.1.0 0.0.0.255** to create the appropriate allow statement. Remember that an access list uses wildcard masks, which are basically inverse sub netmasks.

Type **exit** to leave the access-list configuration mode, and return to global configuration mode.

Configuring the Public Interface:

The following instructions enable the VPN by setting the interface where the crypto engine performs its tasks. This example uses PPP 1 as its Public or WAN interface. The crypto map should always be applied to the Public or WAN interface. You should evaluate your own configuration to determine which interface is your Public or WAN interface.

Type **interface ppp 1** to enter the interface configuration mode.

Type **crypto map VPN** to set this VPN to be used on the interface ppp 1; again you will need to evaluate your own configuration to determine which interface is your public interface.

Configuring the Firewall:

If the firewall in your AOS device is not enabled, your configuration is complete and you should skip this section. The following configuration steps configure the AOS firewall to allow communication across the VPN.

The AOS firewall uses policy-classes to define rules for traffic that enters an interface. You should evaluate your AOS device's configuration to determine which "access-policies" are assigned to your public and your private interfaces. For this example the

access-policy Public will be used for the public interface, and the access-policy Private will be used for the private interface.

Type **ip policy-class Private** to enter the Private policy-class configuration mode. This is the policy-class that is applied to your LAN interfaces.

Type **allow list VPN-10-Selectors** to add a rule that allows traffic for the VPN through the private interface of the firewall. Note that this adds the allow rule to the bottom of the list private policy-class list and that you may have rules already in the Private policy-class that block the traffic for your VPN. You should evaluate each of the rules in your policy-class to make this determination.

Type **exit** to exit the private policy-class and return to global configuration mode.

Type **ip policy-class Public** to enter the Public policy-class configuration mode. This is the policy-class that is applied to your WAN interface.

Type **allow reverse list VPN-10-Selectors** to allow the ‘reverse’ of the VPN selectors through the AOS firewall. The reverse is needed because the access-list VPN-10-Selectors identifies traffic from the local private network to the remote private network and the Public policy class only applies to traffic in the reverse; in other words the Public policy-class applies to traffic from the remote private network to the local private network.

Type **end** to return to privileged mode (enable mode).

Saving the Configuration:

It is important to save the configuration!

Type **write** to save the configuration.

You should create a backup copy of the routers configuration on your computer. To create a backup of the running configuration start a capture of the console output in your telnet or VT100 program; consult the program’s documentation for more information.

Type **show run** at the AOS device’s prompt.

Press **Space Bar** until the end of the running configuration; noted by returning to a command prompt.

Save the output of ‘show run’ as a text file. This text file can later be used to restore the configuration to the router.

Troubleshooting

Troubleshooting a VPN should be performed in this order.

- 1) Attempt to bring up the VPN
- 2) Evaluate the IKE and IPSEC Security Associations
- 3) Evaluate Debug Output

Attempt to bring up the VPN:

The VPN will be automatically initiated when traffic that needs to be transported across the VPN occurs. You can perform this task manually with a ping command from the Command Line interface of your AOS device.

This example uses 10.10.10.1 as the local AOS device's LAN (private) interface and 192.168.1.1 as the remote VPN device's LAN (private) interface. You should evaluate your own VPN to determine the device's respective LAN (private) IP addresses.

Type **ping 192.168.1.1 source 10.10.10.1** to generate traffic that should initiate the VPN.

The VPN will take a few moments to initiate, and then traffic should begin to flow normally. After a few seconds you should see exclamation marks across for ping returns indicating success. Try the above ping twice before moving on. If you do receive exclamation marks, your AOS device is properly configured and the VPN is up.

Evaluate IKE and IPSec Security Associations:

IPSec VPNs using main mode have two phases of negotiation. Phase 1 is IKE. You can view the status of the Phase 1 negotiations between your VPN devices in AOS. If there is an IKE association, move on to Phase 2.

Type **show crypto ike sa** to view the IKE (Phase 1) security association. If there is no security association, the IKE, remote and local IDs or pre-sharedkey on your VPN peers do not match. Double check those settings and retry. It is sometimes normal for the IKE security association to be torn down immediately after IPSec negotiates, and that is acceptable.

Type **show crypto ipsec sa** to view the IPSec (Phase 2) security associations. If there are no associations between your AOS device and the VPN peer, phase 2 failed. You should evaluate the IPSec, and the local and remote networks settings on both of your VPN devices.

If your AOS device shows an IPSec security association, your VPN is up; note that the IKE security association may be torn down immediately after the IPSec security association is established and that is acceptable.

Evaluate Debug Output:

VPN debug output is broken up into sections that detail each message of negotiation between the peers. The beginning of each section starts with a message that reads “received first message” or “sent first message”; or ‘second’ message, etc. A description of the message is shown, and then the AOS devices response to that message.

Type **debug crypto ike** to view the IKE negotiation messages. Note that you may need to reissue the ping command to start IKE negotiation again. The debugs that follow are from the initiating or sending device (device you issued ping from); you may be evaluating the same output from the receiving device.

If after issuing the above debug command and the above ping, you do not see any debug output, your configuration is not correct. Double check that the “crypto map” is applied to the public interface, that the VPN selector access-list is correct, that the correct access-list name is referenced in the “crypto map VPN” section, that you have a default route, or a route pointed to the remote private network out the public interface and that the “ip crypto” command is enabled.

First Message of Main Mode

The first message of main mode is sent by the initiating device. The message includes IKE attribute sets and generally unused vendor IDs. The following is an example output of the first message of main mode of “debug crypto ike”. The important parts of this message have been highlighted in bold.

```
2006.08.08 14:51:53 peer 10.19.233.22: Received first message of main mode
2006.08.08 14:51:53 <POLICY: 101> PAYLOADS: SA,PROP,TRANS,VID,VID,VID
2006.08.08 14:51:53 SA PAYLOAD
2006.08.08 14:51:53 DOI: 1
2006.08.08 14:51:53 Situation: 1
2006.08.08 14:51:53 PROPOSAL PAYLOAD
2006.08.08 14:51:53 Proposal No.: 1
2006.08.08 14:51:53 IANA No. for protocol: ISAKMP (1)
2006.08.08 14:51:53 Size of the variable SPI field: 0
2006.08.08 14:51:53 Number of transforms offered: 1
2006.08.08 14:51:53 TRANSFORM PAYLOAD
2006.08.08 14:51:53 Transform Number: 1
2006.08.08 14:51:53 IANA Transform ID: IKE Key (1)
2006.08.08 14:51:53 TRANSFORM ATTRIBUTES
2006.08.08 14:51:53 SA Attrib: Group Description (4)
2006.08.08 14:51:53 Length: 2
2006.08.08 14:51:53 Value: DH Group 1 (1)
2006.08.08 14:51:53 SA Attrib: Authentication Method (3)
2006.08.08 14:51:53 Length: 2
2006.08.08 14:51:53 Value: Pre-shared Key (1)
2006.08.08 14:51:53 SA Attrib: Encryption Algorithm (1)
2006.08.08 14:51:53 Length: 2
2006.08.08 14:51:53 Value: 3DES (5)
2006.08.08 14:51:53 SA Attrib: Authentication Algorithm (2)
2006.08.08 14:51:53 Length: 2
2006.08.08 14:51:53 Value: MD5 (1)
2006.08.08 14:51:53 SA Attrib: Life Type (11)
2006.08.08 14:51:53 Length: 2
2006.08.08 14:51:53 Value: Seconds (1)
2006.08.08 14:51:53 SA Attrib: Life Time (12)
2006.08.08 14:51:53 Length: 4
2006.08.08 14:51:53 Value: (28800)
```

```

2006.08.08 14:51:53 VID PAYLOAD
2006.08.08 14:51:53 Vendor ID Length: 16
2006.08.08 14:51:53 VENDOR ID HASH IN HEX:
2006.08.08 14:51:53 44 85 15 2D 18 B6 BB CD D..-....
2006.08.08 14:51:53 0B E8 A8 46 95 79 DD CC ...F.y..
2006.08.08 14:51:53 VID PAYLOAD
2006.08.08 14:51:53 Vendor ID Length: 16
2006.08.08 14:51:53 VENDOR ID HASH IN HEX:
2006.08.08 14:51:53 90 CB 80 91 3E BB 69 6E ....>.in
2006.08.08 14:51:53 08 63 81 B5 EC 42 7B 1F .c...B{.
2006.08.08 14:51:53 VID PAYLOAD
2006.08.08 14:51:53 Vendor ID Length: 16
2006.08.08 14:51:53 VENDOR ID HASH IN HEX:
2006.08.08 14:51:53 AF CA D7 13 68 A1 F1 C9 ....h...
2006.08.08 14:51:53 6B 86 96 FC 77 57 01 00 k...wW..

```

If the first message of main mode is continuously repeated, or the second message of main mode is not received, then there is a mismatch in IKE settings between the VPN peers. You can see each of the settings listed, as ‘SA Attrib’. When an AOS device receives the first message of main mode with no matching attribute sets, it will generate an informational response telling the initiating device that no attribute set was selected. The following shows the “no proposal chosen” response message.

```

2006.08.08 14:51:53 ERROR# NO MATCHING ISAKMP PROPOSAL
2006.08.08 14:51:53 SENDING NOTIFY MSG:
2006.08.08 14:51:53 NO_PROPOSAL_CHOSEN
2006.08.08 14:51:53 <POLICY: 101> PAYLOADS: NOTIFY
2006.08.08 14:51:53 NOTIFY PAYLOAD
2006.08.08 14:51:53 DOI: 0
2006.08.08 14:51:53 Protocol Id: 1
2006.08.08 14:51:53 Size of SPI: 16
2006.08.08 14:51:53 Type of notify message: 14
2006.08.08 14:51:53 Notify Type: No Proposal Chosen (14)
2006.08.08 14:51:53 Length of Notification Data: 0
2006.08.08 14:51:53 101: Sent informational exchange message
2006.08.08 14:51:53

2006.08.08 14:51:53 CRYPTO_IKE.NEGOTIATION Xauth is not Enabled
2006.08.08 14:51:53 CRYPTO_IKE.NEGOTIATION 101: IkeSelectIsakmpProposal failed
2006.08.08 14:51:53 CRYPTO_IKE.NEGOTIATION IkeProcessData: IkeIdleProcess failed

2006.08.08 14:51:53 CRYPTO_IKE.NEGOTIATION IkeDeleteIsakmpSA :: Deleting any DPD

```

The following shows the reception of a “no proposal chosen” message by the initiating device. This indicates that the peer device did not having a matching IKE attribute set, and that you should evaluate the IKE settings on both VPN devices.

```

2006.06.18 04:23:20 peer 10.19.233.253: Received informational exchange message
2006.06.18 04:23:20 CRYPTO_IKE.NEGOTIATION IkeInNotifyProcess: NOTIFY TYPE: NO PROPOSAL CHOSEN (14)
2006.06.18 04:23:20 CRYPTO_IKE.NEGOTIATION IkeDeleteIsakmpSA :: Deleting any DPD

```

The following is output when the Local ID of either peer does not match the Remote ID of the other peer. In this case, adjust be sure that the Local ID of one peer matches the Remote ID of the other peer and vice versa.

```

2006.08.17 15:11:22 CRYPTO_IKE.NEGOTIATION IkeInNotifyProcess: NOTIFY TYPE: INVALID ID INFORMATION (18)

```

Second Message of Main Mode:

The second message of main mode is a response to the initiating device that indicates the selected IKE attributes set and includes the receiving devices' vendor ID information. There is very little chance that this message will fail, and therefore is not discussed further in this guide.

Third Message of Main Mode:

The third message of main mode is sent by the initiating device and includes several randomly generated keys for creating a hash of the pre-shared key. There is very little chance that this message will fail and therefore is not discussed further in this guide.

Fourth Message of Main Mode:

The fourth message of main mode is a response to the initiating device, that returns the results of the randomly keyed hash against the pre-shared key and the receiving ends own randomly generated keys for hashing. Again, there is very little chance this message will fail and therefore is not discussed further in this guide.

Fifth Message of Main Mode:

The fifth message of main mode is sent from the initiating device, and is the first encrypted message of the negotiation. The fifth message includes the local ID of the initiating device. The following is an example of the fifth message of main mode.

```
2006.06.18 05:31:55 <POLICY: 100> PAYLOADS: ID,HASH
2006.06.18 05:31:55 ID PAYLOAD
2006.06.18 05:31:55 IANA No. for identifi: 1 -> ID_IPV4_ADDR
2006.06.18 05:31:55 Protocol Id: 0
2006.06.18 05:31:55 Port: 0
2006.06.18 05:31:55 Id Data: 10.19.233.22
2006.06.18 05:31:55 HASH PAYLOAD
```

If the initiating device reports sending the fifth message of main mode, but never receives a response, the pre-shared keys probably do not match. You may also see the following debug message output on the receiving device:

```
2006.08.08 16:04:04 peer 10.19.233.22: Received fifth message of main mode
2006.08.08 16:04:04 decode error
```

If after receiving and correctly decrypting the fifth message of main mode, the receiving device finds that the initiating device's local ID does not match the receiving device's

configured Remote ID the receiving device will responds with a “Invalid ID” notification. The following is an example of that output:

```
2006.08.08 16:18:21 INVALID_ID_INFORMATION
2006.08.08 16:18:21 <POLICY: 101> PAYLOADS: HASH,NOTIFY
2006.08.08 16:18:21 HASH PAYLOAD
2006.08.08 16:18:21 NOTIFY PAYLOAD
2006.08.08 16:18:21 DOI: 0
2006.08.08 16:18:21 Protocol Id: 1
2006.08.08 16:18:21 Size of SPI: 16
2006.08.08 16:18:21 Type of notify message: 18
2006.08.08 16:18:21 Notify Type: Invalid ID Info (18)
2006.08.08 16:18:21 Length of Notification Data: 0
2006.08.08 16:18:21 101: Sent informational exchange message
```

In the same case, the initiating device will receive the “Invalid ID” notification and the output will be as follows:

```
2006.06.18 05:41:56 peer 10.19.233.253: Received informational exchange message
2006.06.18 05:41:56 <POLICY: 100> PAYLOADS: HASH,NOTIFY
2006.06.18 05:41:56 HASH PAYLOAD
2006.06.18 05:41:56 NOTIFY PAYLOAD
2006.06.18 05:41:56 DOI: 0
2006.06.18 05:41:56 Protocol Id: 1
2006.06.18 05:41:56 Size of SPI: 16
2006.06.18 05:41:56 Type of notify message: 18
2006.06.18 05:41:56 Notify Type: Invalid ID Info (18)
2006.06.18 05:41:56 Length of Notification Data: 0
```

You should double check that the local ID of the initiating device matches the configured remote ID of the receiving device.

Sixth Message of Main Mode:

The sixth message of main mode is a response to the initiating device and includes the receiving devices local ID.

```
2006.08.08 16:08:20 <POLICY: 101> PAYLOADS: ID,HASH
2006.08.08 16:08:20 ID PAYLOAD
2006.08.08 16:08:20 IANA No. for identifi: 1 -> ID_IPV4_ADDR
2006.08.08 16:08:20 Protocol Id: 0
2006.08.08 16:08:20 Port: 0
2006.08.08 16:08:20 Id Data: 10.19.233.253
2006.08.08 16:08:20 HASH PAYLOAD
```

If after receiving the sixth message of main mode, the initiating device finds that the remote device’s local ID does not match the initiating device’s configured Remote ID, the IKE negotiations will fail and an “Invalid ID” notification message will be sent to the remote device. The following is an example output of that message from the initiating device:

```
2006.06.18 05:37:41 SENDING NOTIFY MSG:
2006.06.18 05:37:41 INVALID_ID_INFORMATION
2006.06.18 05:37:41 <POLICY: 100> PAYLOADS: HASH,NOTIFY
2006.06.18 05:37:41 HASH PAYLOAD
2006.06.18 05:37:41 NOTIFY PAYLOAD
2006.06.18 05:37:41 DOI: 0
2006.06.18 05:37:41 Protocol Id: 1
```

```
2006.06.18 05:37:41 Size of SPI: 16
2006.06.18 05:37:41 Type of notify message: 18
2006.06.18 05:37:41 Notify Type: Invalid ID Info (18)
2006.06.18 05:37:41 Length of Notification Data: 0
2006.06.18 05:37:41 100: Sent informational exchange message
```

You should double check that the remote device's Local ID matches the initiating device's configured Remote ID.

With the transmission of the fifth and sixth messages of main mode, and the absence of a notification message, IKE negotiation is considered complete. Both peers will display the same message.

```
2006.06.18 05:46:54 peer 10.19.233.253: Main mode completed
```

Debugging IPsec:

Type **debug crypto ipsec** to begin debugging IPsec negotiations. IPsec negotiations are commonly known as "quick mode". There are four messages in quick mode that identify the IPsec attributes and the networks to be connected.

After issuing the above debug command you may need to issue the ping 'source' command to start the negotiations again.

First Message of Quick Mode:

The first message of quick mode is sent from the initiating device. The first message of quick mode includes IPsec attributes, and source and destination networks. The following is an example output of the first message of quick mode.

```
2006.06.18 05:46:54 100: Sent first message of quick mode
2006.06.18 05:46:54 <POLICY: 100> PAYLOADS: HASH,SA,PROP,TRANS,NONCE,ID,ID,KE
2006.06.18 05:46:54 HASH PAYLOAD
2006.06.18 05:46:54 SA PAYLOAD
2006.06.18 05:46:54 DOI: 1
2006.06.18 05:46:54 Situation: 1
2006.06.18 05:46:54 PROPOSAL PAYLOAD
2006.06.18 05:46:54 Proposal No.: 1
2006.06.18 05:46:54 IANA No. for protocol: IPsec ESP (3)
2006.06.18 05:46:54 Size of the variable SPI field: 4
2006.06.18 05:46:54 Number of transforms offered: 1
2006.06.18 05:46:54 SPI for the proposal: 4059201966
2006.06.18 05:46:54 TRANSFORM PAYLOAD
2006.06.18 05:46:54 Transform Number: 1
2006.06.18 05:46:54 IANA Transform ID: 3DES (3)
2006.06.18 05:46:54 TRANSFORM ATTRIBUTES
2006.06.18 05:46:54 SA Attrib: Authentication Algorithm (5)
2006.06.18 05:46:54 Length: 2
2006.06.18 05:46:54 Value: SHA1 (2)
2006.06.18 05:46:54 SA Attrib: Group Description (3)
2006.06.18 05:46:54 Length: 2
2006.06.18 05:46:54 Value: Unknown/Other (1)
2006.06.18 05:46:54 SA Attrib: Encapsulation Mode (4)
2006.06.18 05:46:54 Length: 2
2006.06.18 05:46:54 Value: Tunnel (1)
2006.06.18 05:46:54 SA Attrib: Life Type (1)
2006.06.18 05:46:54 Length: 2
```



```

2006.06.18 05:46:54      Value: Seconds (1)
2006.06.18 05:46:54      SA Attrib: Life Time (2)
2006.06.18 05:46:54      Length: 4
2006.06.18 05:46:54      Value: (28800)
2006.06.18 05:46:54      NONCE PAYLOAD
2006.06.18 05:46:54      ID PAYLOAD
2006.06.18 05:46:54      IANA No. for identifi: 4 -> IPV4_ADDR_SUBNET
2006.06.18 05:46:54      Protocol Id: 0
2006.06.18 05:46:54      Port: 0
2006.06.18 05:46:54      Id Data: 10.10.10.0, 255.255.255.0
2006.06.18 05:46:54      ID PAYLOAD
2006.06.18 05:46:54      IANA No. for identifi: 4 -> IPV4_ADDR_SUBNET
2006.06.18 05:46:54      Protocol Id: 0
2006.06.18 05:46:54      Port: 0
2006.06.18 05:46:54      Id Data: 192.168.1.0, 255.255.255.0
2006.06.18 05:46:55      KE PAYLOAD

```

If the IPSec attributes of the VPN devices do not match, an information exchange message “No Proposal Chosen” will be sent to the initiating device. The following is the debug output of the initiating device.

```

2006.06.18 05:59:07 peer 10.19.233.253: Received informational exchange message
2006.06.18 05:59:07 <POLICY: 100> PAYLOADS: HASH,NOTIFY
2006.06.18 05:59:07      HASH PAYLOAD
2006.06.18 05:59:07      NOTIFY PAYLOAD
2006.06.18 05:59:07      DOE: 1
2006.06.18 05:59:07      Protocol Id: 3
2006.06.18 05:59:07      Size of SPI: 4
2006.06.18 05:59:07      Type of notify message: 14
2006.06.18 05:59:07      SPI: 3667199196
2006.06.18 05:59:07      Notify Type: No Proposal Chosen (14)
2006.06.18 05:59:07      Length of Notification Data: 0
2006.06.18 05:59:07 RECEIVED NOTIFY MSG:
2006.06.18 05:59:07 NO_PROPOSAL_CHOSEN

2006.06.18 05:59:07 CRYPTO_IKE.NEGOTIATION
2006.06.18 05:59:07 CRYPTO_IKE.NEGOTIATION IkeInNotifyProcess: NOTIFY TYPE: NO PROPOSAL CHOSEN (14)

```

If after sending the first message of quick mode, there is no response, the networks to be transported do not match. The receiving device will display the following message:

```

2006.08.08 16:31:52 CRYPTO_IKE.NEGOTIATION The remote ID specified IPSec Policy "VPN 10", but the selectors did not match

```

You should double check both the source and destination networks (command line access-list) on both of your VPN devices. The source network of one device should match the destination network of the other; and vice-versa.

Second Message of Quick Mode:

The second message of quick mode is a response to the initiating device that identifies the selected attributes and the IP Networks to be transported. There is very little chance that the second message of quick mode will fail, and therefore is not discussed further.

Third & Fourth Messages of Quick Mode:

The third and fourth messages of quick mode are acknowledgements of the IPSec association and represent the final messages. There is very little chance that these messages will fail.

Type **undebug all** to turn off IKE and IPSec debugging output.

I have done all of the above troubleshooting, but I am still unable to ping.

If after completing the VPN configuration, and successfully establishing an IPSec security association, shown in the output of “show crypto ipsec sa” you are still unable to pass traffic, check the firewall settings on both VPN devices. There should be a specific rule on both interfaces of the AOS device that allow VPN traffic through that interface.

Please also double check the default gateway settings of the computers connected to the private networks. The default gateway of any device that will use the VPN should be the AOS device’s private (LAN) ip address.