



Creating a Gateway to Client VPN between Sidewinder G2[®] and a Mac[®] OS X Client

*This application note describes how to
set up a VPN connection between a
Mac client and a Sidewinder G2
Security Appliance using VPN Tracker.*

Table of Contents

Overview	3
Preparing the gateway and client	4
Preparing the Sidewinder G2 gateway	4
Preparing the Mac client	4
Configuring Sidewinder G2	5
Configuring Sidewinder G2	5
Configuring VPN Tracker for shared key	10
Configuring VPN Tracker for certificates	19
Troubleshooting tips	23

Overview

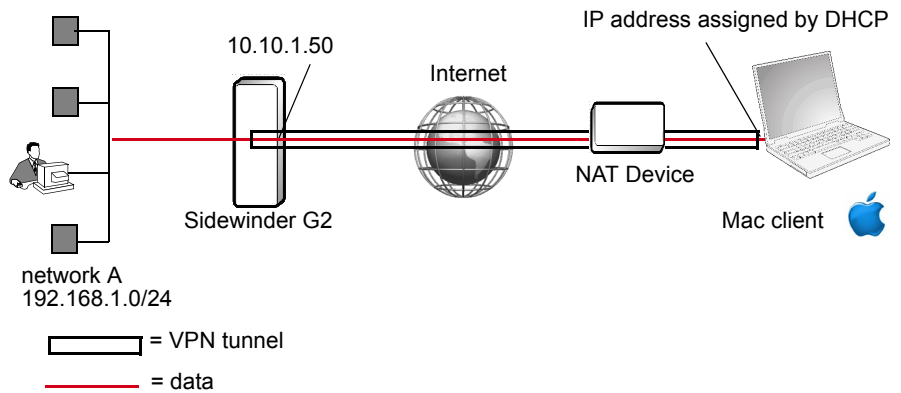
Sidewinder G2 Security Appliance's VPN implementation is based on the well-defined IPsec and ISAKMP protocols, giving it the ability to establish VPN connections with a wide variety of clients, operating systems, and devices. This application note describes how to set up an IPsec VPN connection between a Mac client and a Sidewinder G2 Security Appliance using VPN Tracker.

This document includes two scenarios for the Mac client:

- Mac client to Sidewinder using a shared key
- Mac client to Sidewinder using certificates

Both scenarios describe how to set up a gateway-to-client VPN connection between a Mac OS X client and a Sidewinder G2. The configuration presented here is a basic configuration. Both scenarios assume that the Mac client has a dynamic IP address and is behind a NAT device. Figure 1 shows a network diagram of this scenario.

Figure 1: Gateway to gateway, fixed IP VPN



Preparing the gateway and client

Before setting up the VPN between your Sidewinder G2 gateway and Mac client, each system must meet the requirements specified here.

Preparing the Sidewinder G2 gateway

This configuration is assumed to work with all 6.1.x.xx versions, but has not been thoroughly tested on all version or configurations.

Before creating the necessary Security Associations, do the following:

- Enable the ISAKMP server in the appropriate burbs (**Services Configuration > Servers > ISAKMP**).
- Create a rule allowing inbound ISAKMP traffic to the ISAKMP server (**Policy Configuration > Rules**).

You should also plan out this VPN's security policy. See the VPN chapter of the *Sidewinder G2 Administration Guide* and the "Configuring a VPN when using Proxy and IP Filter Rules" application note for more information. They can be found at kb.securecomputing.com.

Preparing the Mac client

Other Mac VPN clients exist, however we recommend the VPN Tracker client based on its features and security.



Important: *Secure Computing only supports the Sidewinder G2 end of this VPN. For problems with VPN Tracker, please contact Equinix support.*

Equinix VPN Tracker

- Supports using certificates and extended authentication (XAUTH), as well as shared password. For more information and to download a free trial, see <http://www.equinix.com/vpntracker>.
- We recommend using VPN Tracker version 4.9.1 or newer as it comes with a Sidewinder G2 profile.

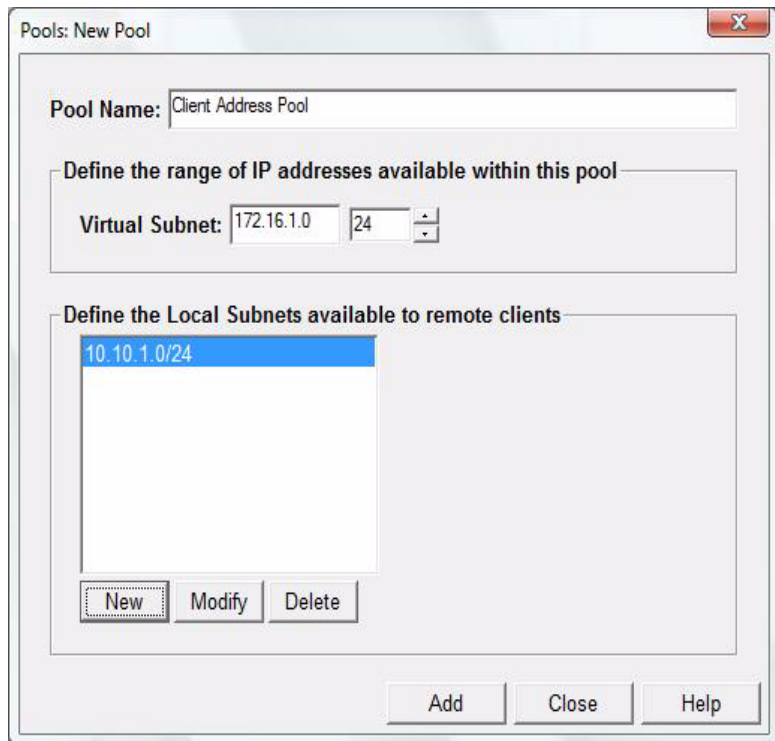
Configuring Sidewinder G2

This section covers the parameters that need to be set on each end of the gateway-to-client VPN.

Configuring Sidewinder G2

You will need to ensure client address pools are defined in the Sidewinder G2. Client address pools are used to manage VPN connections between clients and the Sidewinder G2. When a client attempts a connection, the Sidewinder G2 assigns an IP address from an administrator-defined pool. The Sidewinder G2 negotiates with the client to determine other requirements, such as DNS or WINS servers. If successful, a connection is established. For more information on client address pool, see the VPN chapter of the *Sidewinder G2 Administration Guide* found at www.securecomputing.com/goto/manuals.

- 1 Log into the Admin Console.
- 2 Select **VPN Configuration > Client Address Pools**. The following window appears.



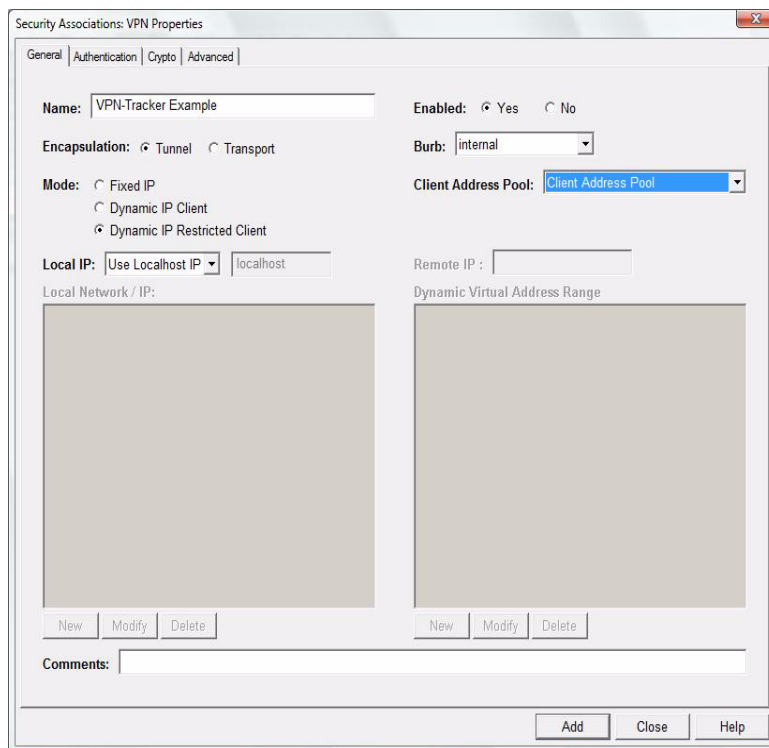
This window allows you to create and modify client address pools.

- 3 Enter the range of IP addresses for the virtual subnet that will be assigned to the VPN client.
- 4 Define your local subnet that the client will be able to access.

At this point, your ISAKMP server should be enabled and its associated rule should be active. The next step is to create a new Security Association for this VPN by doing the following:

- 1 Log into the Admin Console.
- 2 Select **VPN Configuration > Security Associations**.
- 3 Click **New**. A window similar to the following appears.

Figure 2: Security Association General tab for the example VPN



- 4 On the General tab, enter the following information:

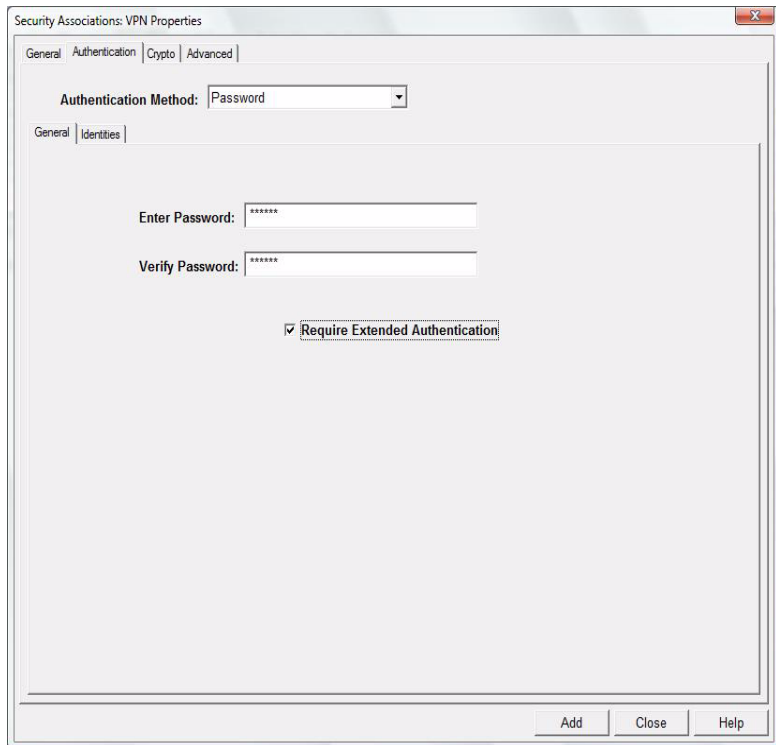
Field Name	Value
Name	site specific
Enabled	Yes
Encapsulation	Tunnel

More...

Field Name	Value
Burb	<i>site specific</i>
Mode	Dynamic IP Restricted Client
Client Address Pool	<i>site specific</i>
Local IP	Use Localhost IP
Local Network/IP	Defined by client address pool
Remote IP	NA
Remote Network/IP	NA

- 5 On the Authentication tab, you can use either the shared key or certificate method.
 - If using shared key see step 6.
 - If using certificates, see step b on page 7.
- 6 For shared key, select **Password** as the Authentication Method. The following window appears.

Figure 3: Shared key Authentication tab's General sub-tab for the example VPN



- a On the General sub-tab, enter and confirm a password. This password

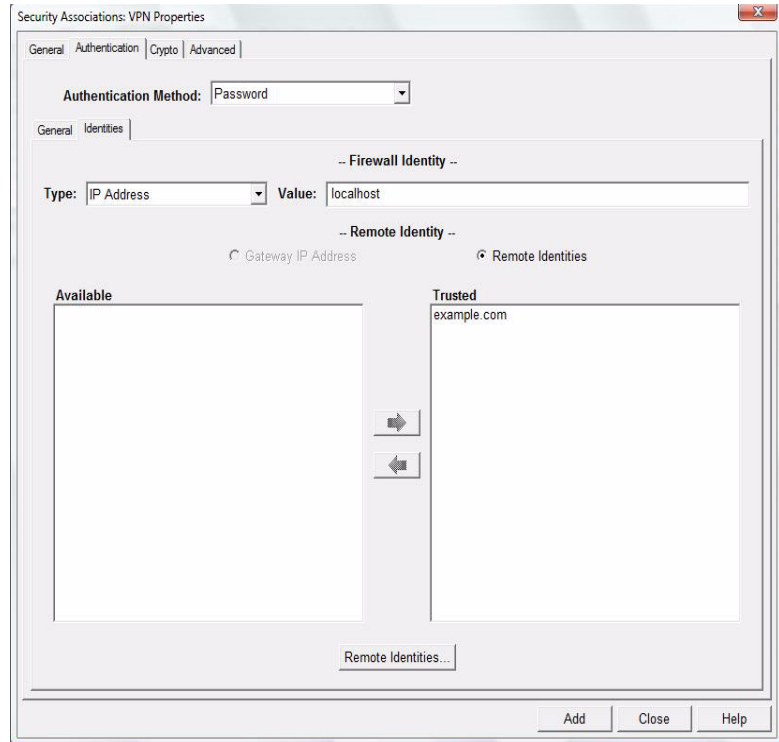
is to be shared with the administrator of the Mac client.

b [Optional] Select **Require Extended Authentication**.

Note: With shared key, we recommend using the Require Extended Authentication option for added security.

c Click the Identities sub-tab. A window similar to the following appears:

Figure 4: Shared key Authentication tab's Identities sub-tab for the example



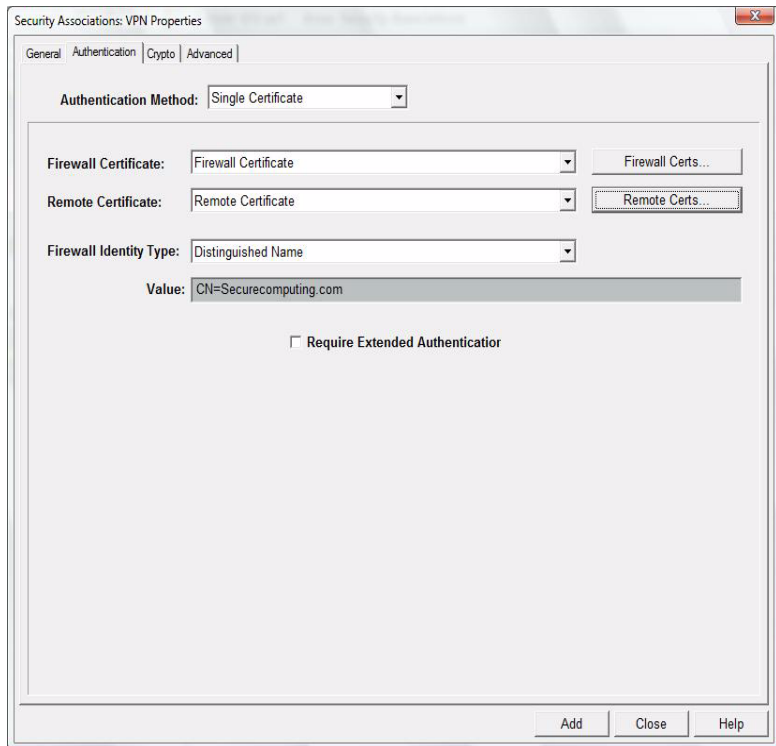
d On the Identities sub-tab, do the following:

- Verify that you correctly entered the Firewall Identity on the General tab. In the example, this would be Type = IP Address, Value = localhost.
- Set the Remote Identity: Trusted as the client's domain name (the one entered in VPN Tracker). If this remote identity does not currently exist, click **Remote Identities**. If you need more information, see the online help.

In the example, this is *example.com*.

- 7 For certificates select **Single Certificate** as the Authentication Method. The following window appears.

Figure 5: Certificates Authentication tab's General sub-tab for the example VPN



- a Select **Firewall Certificate** for the Firewall Certificate. To create, view, or modify certificates, click Firewall Certs.
 - b Select **Remote Certificate** for the Remote Certificate. To create, view, or modify certificates, click Remote Certs.
 - c Select **Distinguished Name** for the Firewall Identity Type.
 - d Enter the common name for the Value.
 - e [Optional] Select **Require Extended Authentication**.
- 8 On the Crypto and Advanced tabs, you may leave the default values. If you plan to use algorithms other than 3DES and SHA1 (the defaults), configure the new values on the Crypto tab. The values on the Advanced tab rarely need modification.
 - 9 Click **Add**.
 - 10 Click the **Save** icon to save the new Security Association.

The Sidewinder G2 side of the VPN is now configured. Continue in the appropriate section:

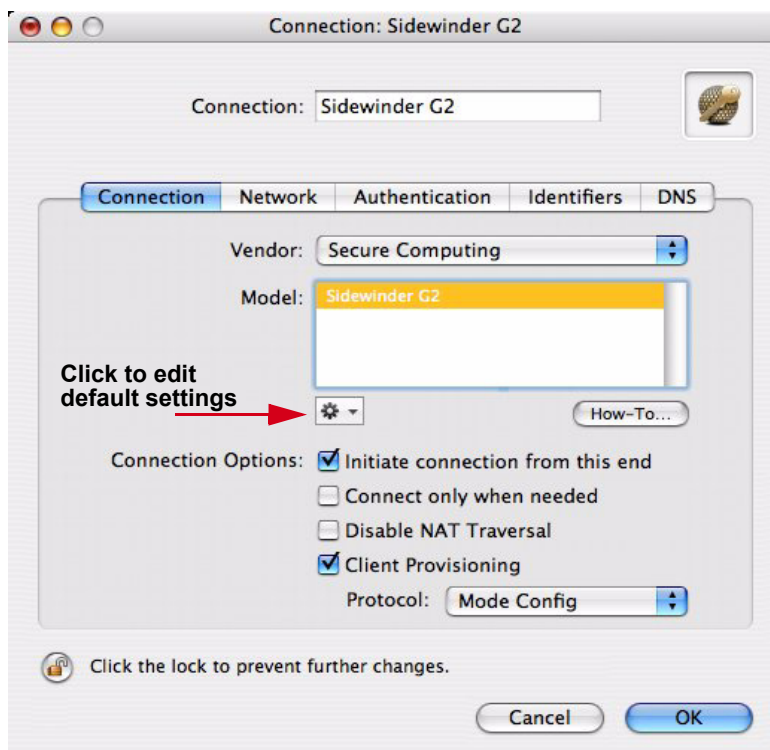
- “Configuring VPN Tracker for shared key” on page 10
- “Configuring VPN Tracker for certificates” on page 19

Configuring VPN Tracker for shared key

If you are using VPN Tracker with a shared key, do the following:

- 1 Start VPN Tracker and click **New**. The following window appears.

Figure 6: VPN Tracker
New window



- 2 On the Connection tab, enter parameters for this connection:

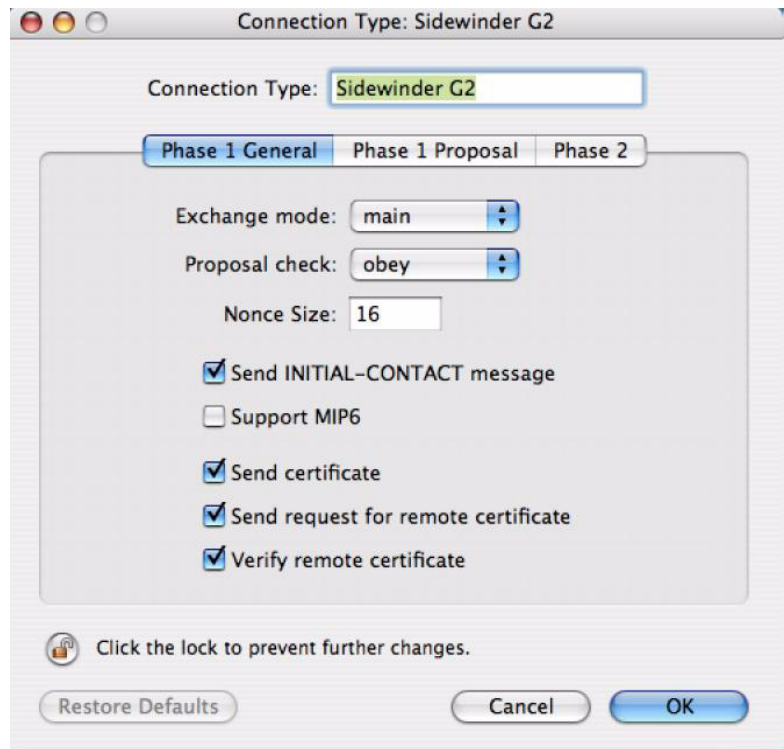
Field Name	Value
Connection	Enter a name that identified this connection, such as <i>Sidewinder</i> .
Vendor	Select Secure Computing.

More...

Field Name	Value
Model	Use Sidewinder G2, which is the default. For more information, see step a.
Connection Options	<ul style="list-style-type: none"> • Initiate connection from this end • Client Provisioning • Protocol: Mode Config <p>Mode Config is an Internet Key Exchange (IKE) extension that enables the IPSec VPN gateway to provide LAN configuration information to the remote user's machine. This allows Sidewinder G2 to assign a virtual IP address to the client from the Client Address Pool, as well as DNS and WINS server settings if required.</p>

- a If you need to modify or view the default settings, click the icon below the Model field, or double-click the model name.

Figure 7: VPN Tracker Sidewinder G2 default settings

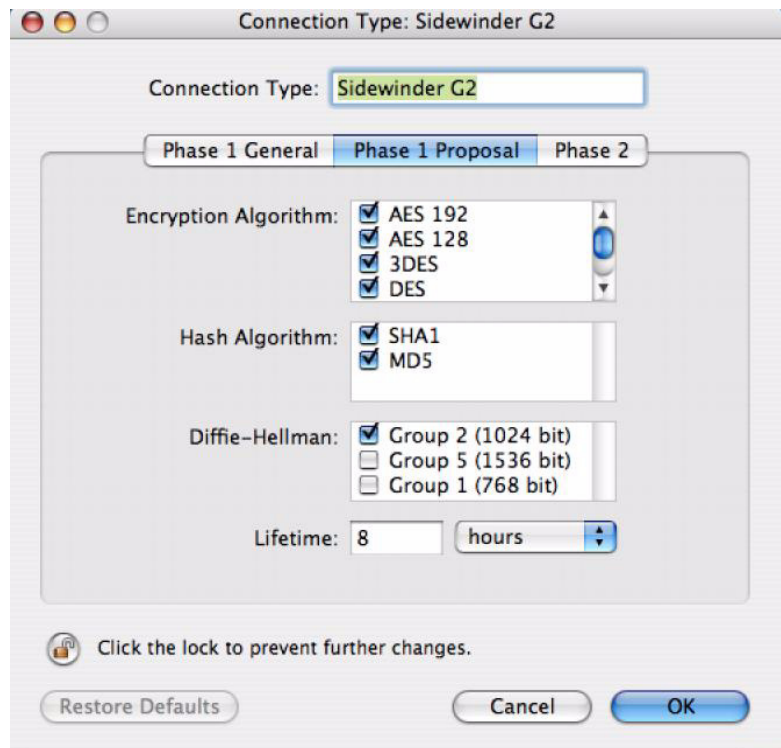


b On the Phase 1 General tab, verify the default settings are as follows:

Field Name	Value
Connection Type	Sidewinder G2
Exchange Mode	Main
Proposal Check	obey
Nonce Size	16
Additional options	<ul style="list-style-type: none"> • Send INITIAL-CONTACT message • Send certificate • Send request for remote certificate • Verify remote certificate

c Select the **Phase 1 Proposal** tab. The following window appears.

Figure 8: VPN Tracker
Phase 1 Proposal tab

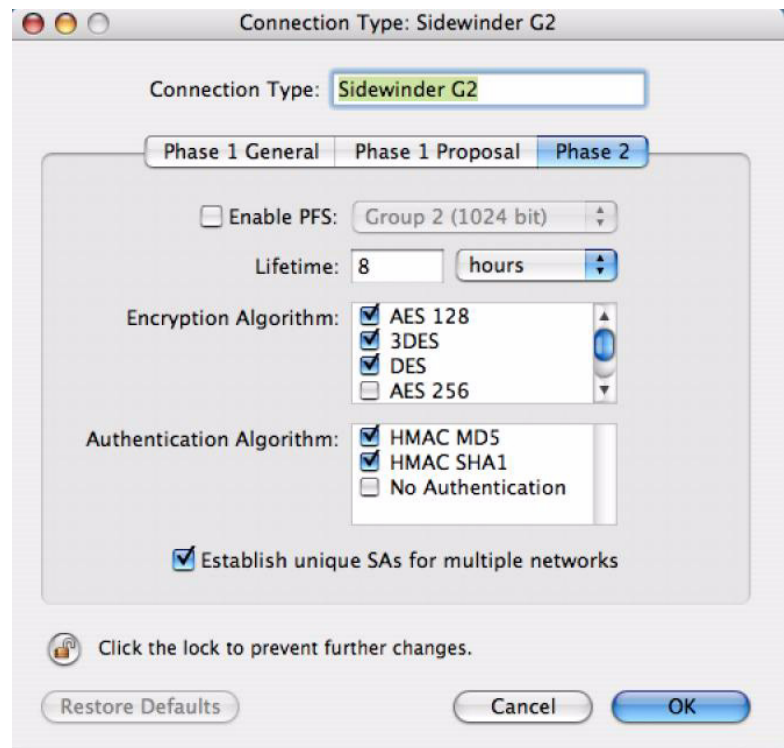


- d On the Phase 1 Proposal tab, verify the default settings are as follows:

Field Name	Value
Encryption Algorithm	Match to the encryption algorithm used in the corresponding Sidewinder G2 Security Association, all algorithms are selected by default.
Hash Algorithm	Match to the hash algorithm used in the corresponding Sidewinder G2 Security Association. The defaults are SHA1 and MDS.
DH Group	Group 2 (1024 bit) is the default, other groups may be used if configured on Sidewinder. May also use modp1536
Lifetime	This is set to 8 hours by default, the recommend Lifetime is 1 hour .

- e Select the **Phase 2** tab. The following window appears.

Figure 9: VPN Tracker Phase 2 window



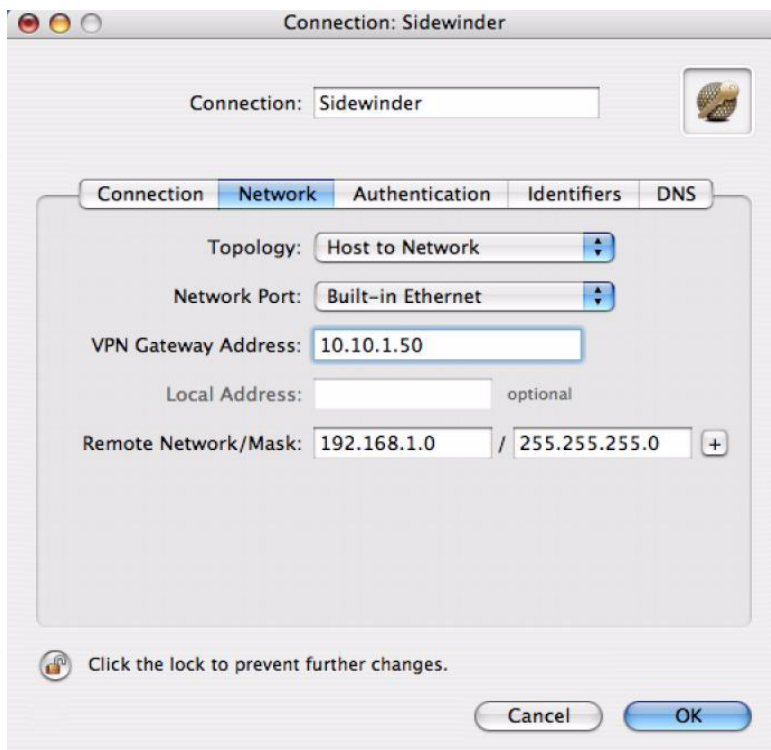
- f On the Phase 2 tab, verify the default settings are as follows:

Field Name	Value
PFS Group	By default this is not enabled on Sidewinder. Select this option only if it has been enabled on Sidewinder.
Lifetime	8 hours (default) If necessary, the client will set this to match Sidewinder G2's phase 2 lifetime value.
Encryption Algorithms	Match to the algorithms set in the corresponding Sidewinder G2 Security Association, or keep the defaults.
Authentication Algorithms	Match to the algorithms set in the corresponding Sidewinder G2 Security Association. Sidewinder G2 supports both MD5 and SHA1, which are the defaults.
Establish unique SAs for multiple networks	Leave blank if you have multiple networks and want them to use the same SA.

- g Click **OK** to save changes or to keep the default settings. Continue configuring the connection.

- 3 If it is not already selected, select the **Network** tab. The following window appears.

Figure 10: VPN Tracker Network tab

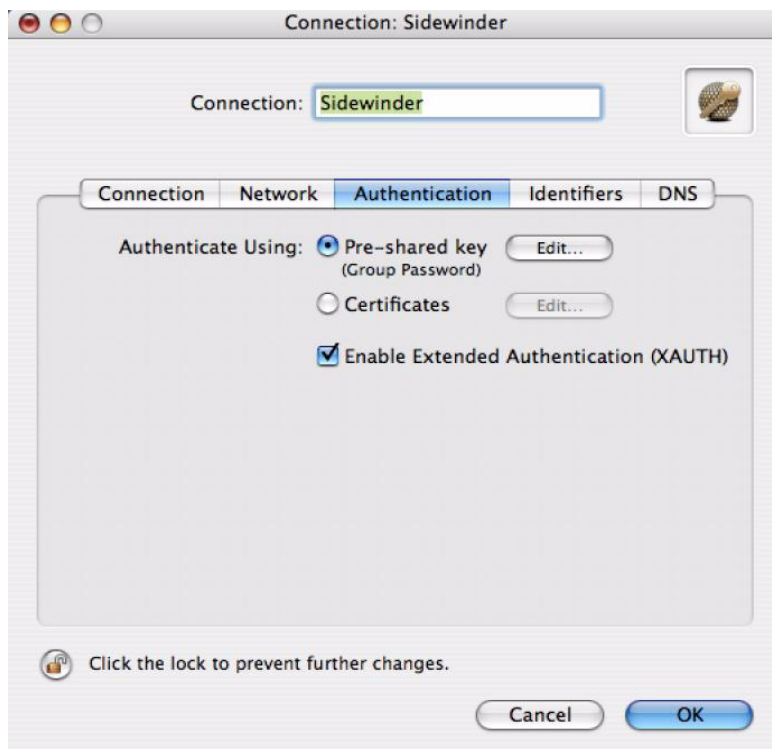


- 4 On the Network tab, set the network parameters that will make up the VPN connection:

Field Name	Value
Topology	Host to Network
Network Port	Site dependent If you do not want to specify which network port this VPN should use, select Automatic .
VPN Gateway Address	The Sidewinder G2's IP address to which this VPN will connect, generally the Sidewinder G2's external address. If Figure 1 on page 3, this is 10.10.1.50.
Local Address	Leave blank
Remote Network/Mask	Network address and netmask of Sidewinder G2's internal network this client will access over the VPN. If Figure 1 on page 3, this is 192.168.1.0/24.

5 Select the **Authentication** tab. The following window appears.

Figure 11: VPN Tracker
Authentication tab



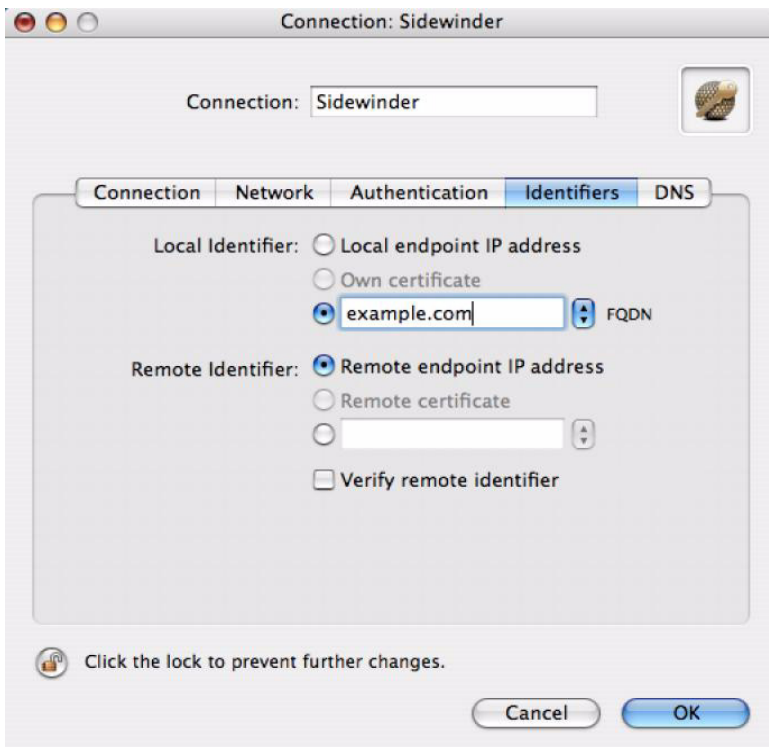
- a You can use either Pre-shared key or Certificates.
- If using Pre-shared key continue to step 6.
 - If using certificates, skip to the section “Configuring VPN Tracker for certificates” on page 19.

6 On the Authentication tab, set the authentication method to use between the VPN Tracker and the Sidewinder G2:

Field Name	Value
Authentication Using	Pre-shared key
Enable Extended Authentication (XAUTH)	Enabled (recommended). This must be also configured on Sidewinder.

7 Select the **Identifiers** tab. The following window appears.

Figure 12: VPN Tracker Identifiers tab



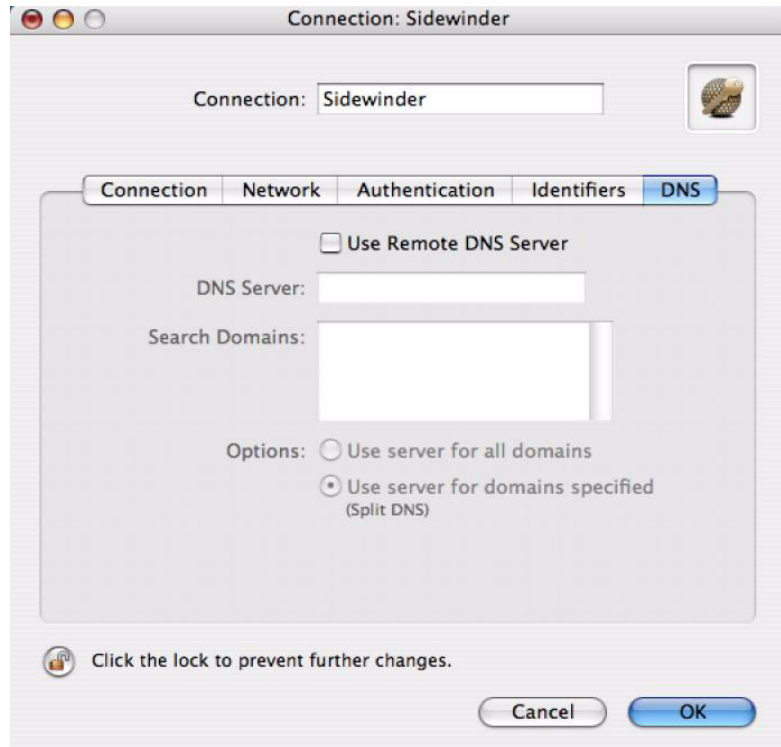
8 On the Identifiers tab, set the identifiers:

Field Name	Value
Local Identifier	<p>Use FQDN if address or e-mail is configured for remote identity on Sidewinder.</p> <p>Enter the value this client will use to identify itself to the Sidewinder G2. This value must match the remote identity in the corresponding Sidewinder G2 Security Association.</p> <p>If you select "Address" the client will use its address as its identity. If this is a dynamic connection, the address could change and no longer match the corresponding Sidewinder G2 value.</p>
Remote Identifier	<p>Address in a client-to-gateway VPN.</p> <p>In a client-to-gateway VPN, use the gateway's IP address as the remote identifier. This must match the Security Association's Firewall Identifier.</p>

More...

9 Select the **DNS** tab. The following window appears.

Figure 13: VPN Tracker
DNS tab



Use this area to configure the DNS server to be used by this client. This may also be configured as part of the client address pool on Sidewinder, see the VPN chapter of the *Sidewinder G2 Administration Guide* for more information.

Note: Since this is not directly related to the VPN connection with Sidewinder G2, none of the VPN Tracker DNS settings were tested.

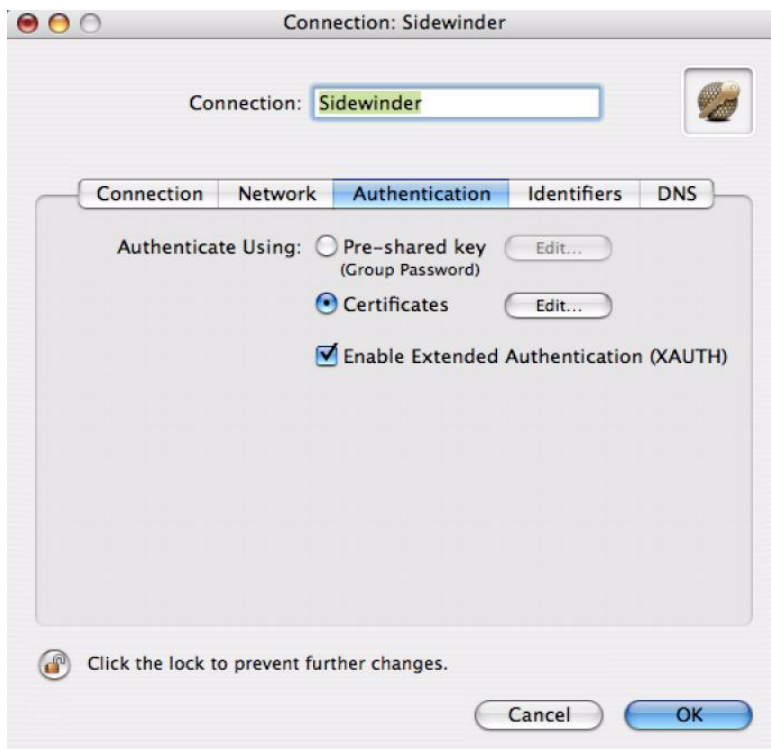
10 Click **OK**.

You have finished configuring the VPN connection for shared key.

Configuring VPN Tracker for certificates

11 Select the **Authentication** tab. The following window appears.

Figure 14: VPN Tracker Authentication tab



12 On the Authentication tab, set the authentication method to use between the Mac OS client and the Sidewinder G2:

Field Name	Value
Authentication Using	Certificates
Enable Extended Authentication (XAUTH)	Enabled (recommended). This must be also configured on Sidewinder.

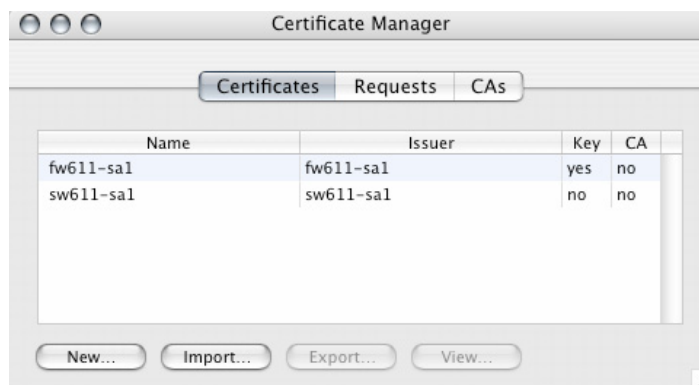
- 13 Click **Edit** to select your certificates. The following window appears. If you do not have any certificates loaded, go to the next step.

Figure 15: VPN Tracker certificates menu



- 14 Click **Edit Certificates** to bring up the Certificate Manager. The following window appears.

Figure 16: VPN Tracker Certificate Manager Certificates tab



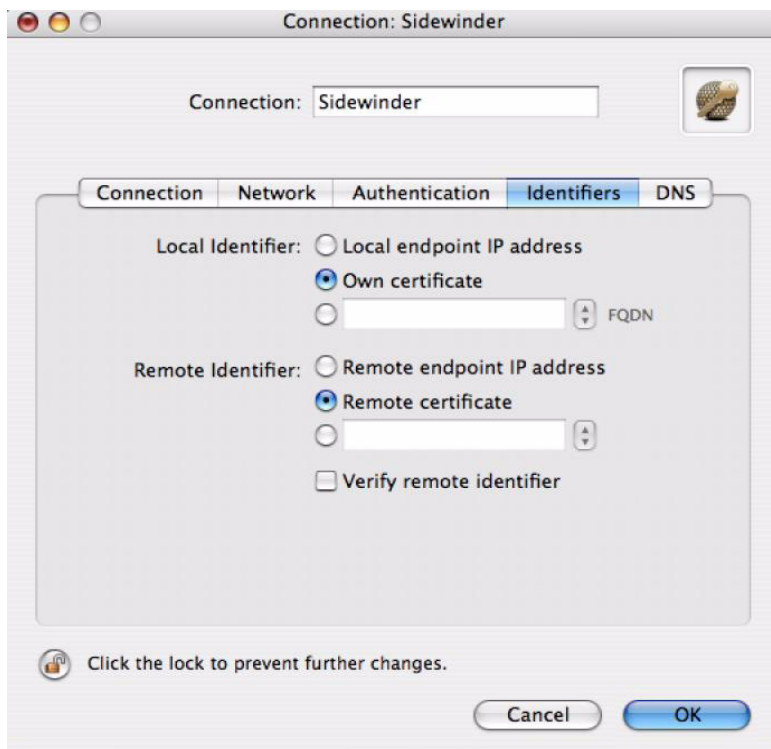
This VPN will require two certificates exported from Sidewinder G2 and imported into this VPN Tracker. Import the following:

- a A remote certificate and its private key
Create this certificate using the Sidewinder G2 Admin Console in the **Services Configuration > Certificate Management > Remote Certificates** area.
- b A firewall certificate only
Create this certificate using the Sidewinder G2 Admin Console in the **Services > Certificate Management > Firewall Certificates** area.

In the *Sidewinder G2 Administration Guide*, see the VPN chapter's section on certificate management.

15 Select the **Identifiers** tab. The following window appears.

Figure 17: VPN Tracker Identifiers tab



16 On the Identifiers tab, set the identifiers:

Field Name	Value
Local Identifier	Own certificate
Remote Identifier	Remote certificate

17 Select the **DNS** tab. The following window appears.

Figure 18: VPN Tracker
DNS tab



Use this area to configure the DNS server to be used by this client. This may also be configured as part of the client address pool on Sidewinder, see the VPN chapter of the *Sidewinder G2 Administration Guide* for more information.

This example is using Mode Config, therefore these settings could be configured as part of the Client Address Pool.

Note: *Since this is not directly related to the VPN connection with Sidewinder G2, none of the DNS settings were tested.*

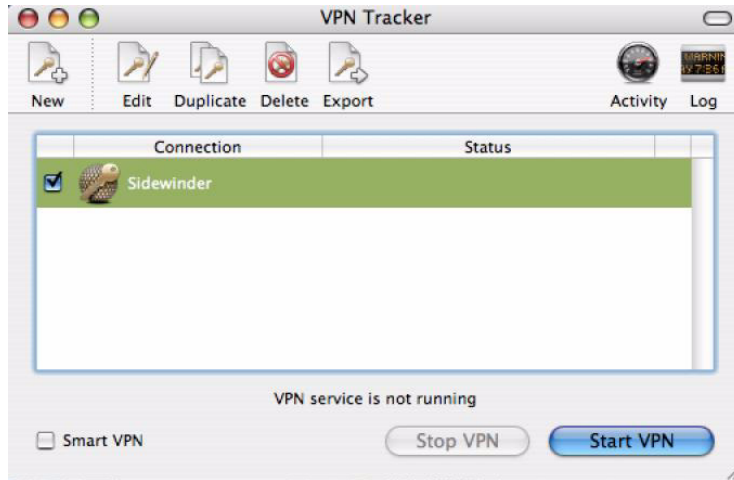
18 Click **OK**.

You have finished configuring the VPN connection for certificates.

Using VPN Tracker

Return to the window shown in Figure 19 to start and stop the VPN and check its connection status.

Figure 19: VPN Tracker main window



Troubleshooting tips

If you are having difficulties getting the VPN connection to work, try some of these basic troubleshooting procedures:

- In the VPN Tracker main window, click the Log button in the upper right-hand corner.
- Ping the gateway (Sidewinder G2's external address) to make sure that you have connectivity between the client and gateway. Ping must be enabled on the gateway first.
- Using a command line session with Sidewinder G2, display live auditing of the VPN connection by entering `showaudit -kv`.
- If you would like to see more detailed auditing, do the following:
 - a Using the Admin Console, select **VPN Configuration > ISAKMP Server**.
 - b Set the Audit Level to **Verbose**. This will show more detailed information on the connection.
- Use these other useful Sidewinder G2 commands for troubleshooting the VPN connection:
 - `cf ipsec status`
 - `cf ipsec reload`
 - `cf ipsec policydump`
 - `cf server restart isakmp`
- Ping device in internal network on other side of VPN tunnel

Product names used within are trademarks of their respective owners.

Copyright © 2007 Secure Computing Corporation. All rights reserved.