

## **SonicWALL VPN Deployment using RADIUS and SecurID**

Tech note prepared by SonicWALL, Inc.

SonicWALL, Inc.  
1160 Bordeaux Drive  
Sunnyvale, CA  
408-745-9600

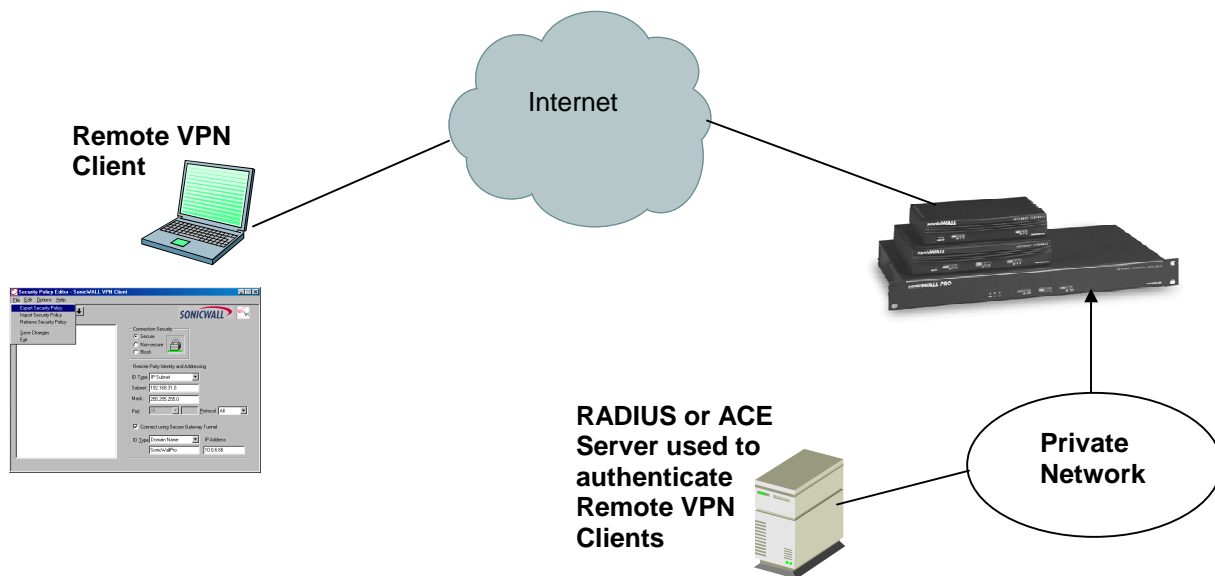
## The Motivation to use RADIUS or SecurID® with SonicWALL VPN Gateway

RADIUS and SecurID enables network administrators effectively deploy and manage VPN Client based remote users.

The RADIUS/ACE server enforces a unique username/password for each user, which allows multiple users to share one VPN Client configuration. This one VPN Client configuration is easily distributed among end-users and reduces configuration headaches associated with multiple VPN Clients.

**Tech Tip:** Security Association (SA) is information shared on both sides of a VPN tunnel. This information allows the two sides of the VPN tunnel establish a secure connection over the public Internet.

## An Example of a Network Configuration



## To Configure the SonicWALL to Communicate with the RADIUS or ACE Server

Log into the SonicWALL Administrator web management screen shown below and select the enable RADIUS checkbox.

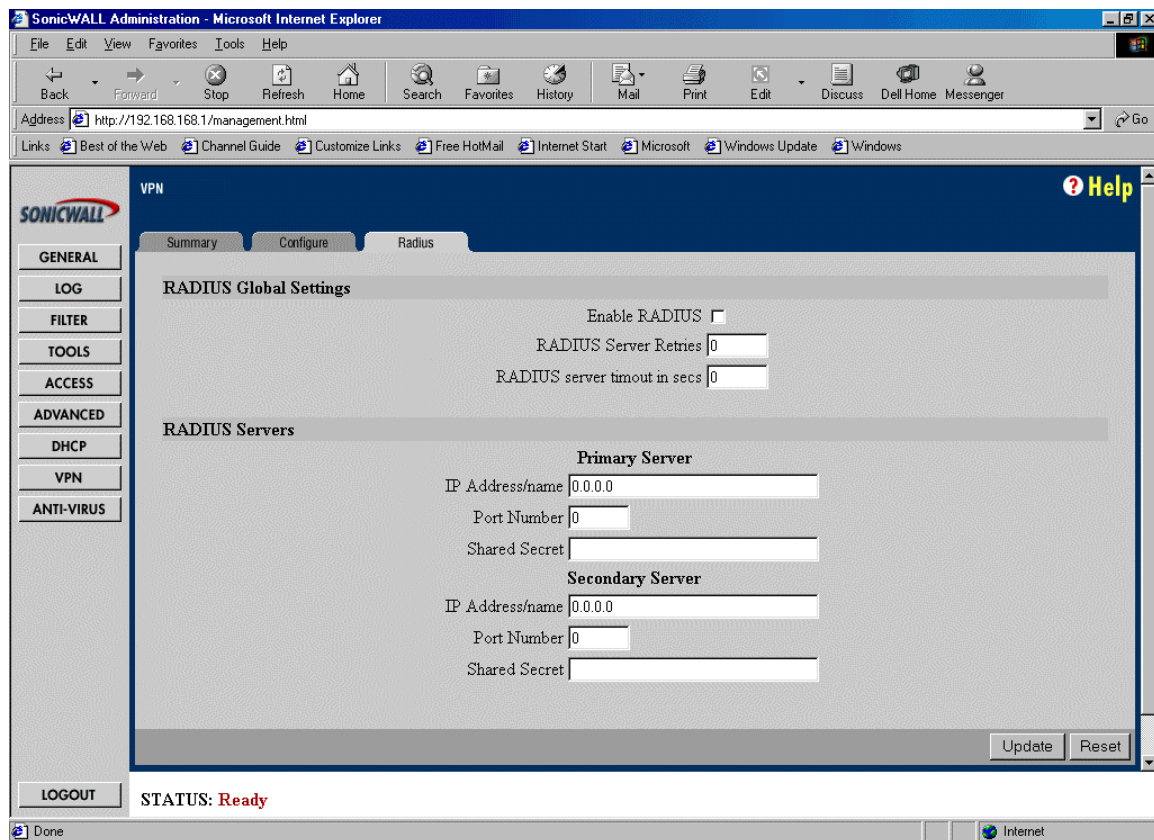
Define the number of times the SonicWALL will attempt to contact the RADIUS/ACE server in the RADIUS Server Retries field. If the RADIUS/ACE does not respond within the specified number of retries, the VPN negotiation is dropped. This field may range between 0 and 30, however 3 is recommended.

Enter the number of seconds between attempts to contact the RADIUS/ACE server in the RADIUS Server Timeout in Seconds field. The RADIUS server timer may range from 0 to 60 seconds, but 5 seconds is recommended.

Specify the IP address of the RADIUS/ACE server in the IP Address/name field.

Enter the UDP port number that the RADIUS/ACE server listens on. The Steel-Belted RADIUS server is set by default to listen on port 1645.

Enter the RADIUS/ACE server's administrative password or "shared secret". This field is case sensitive.

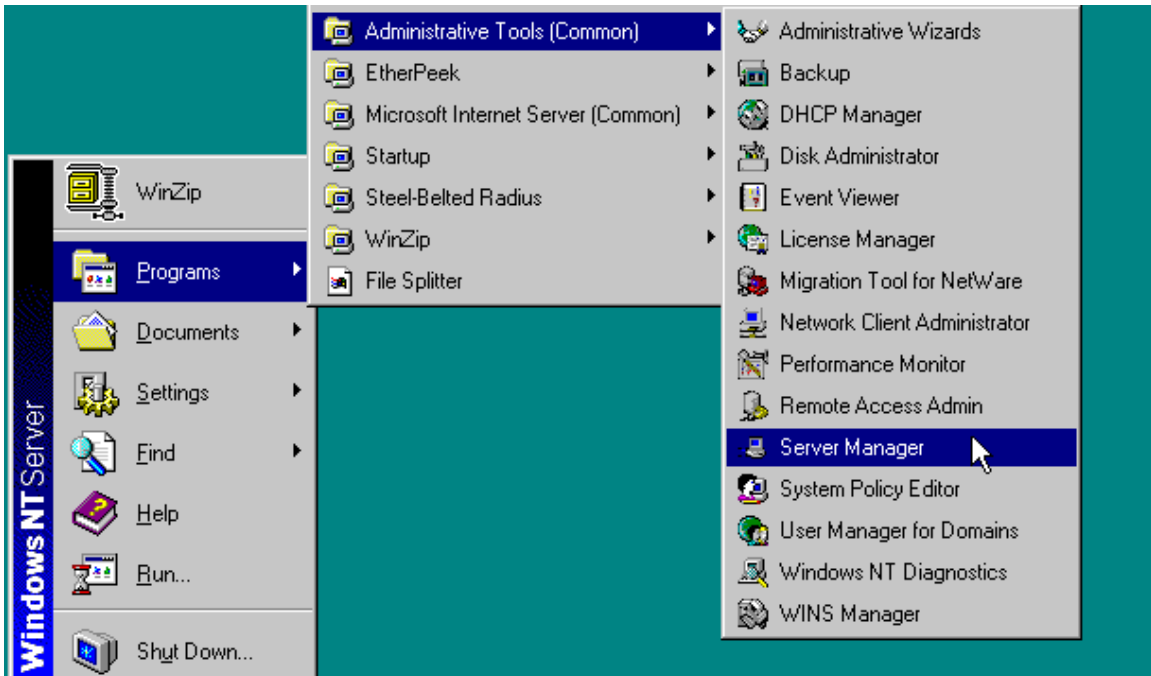


## RADIUS Server Configuration

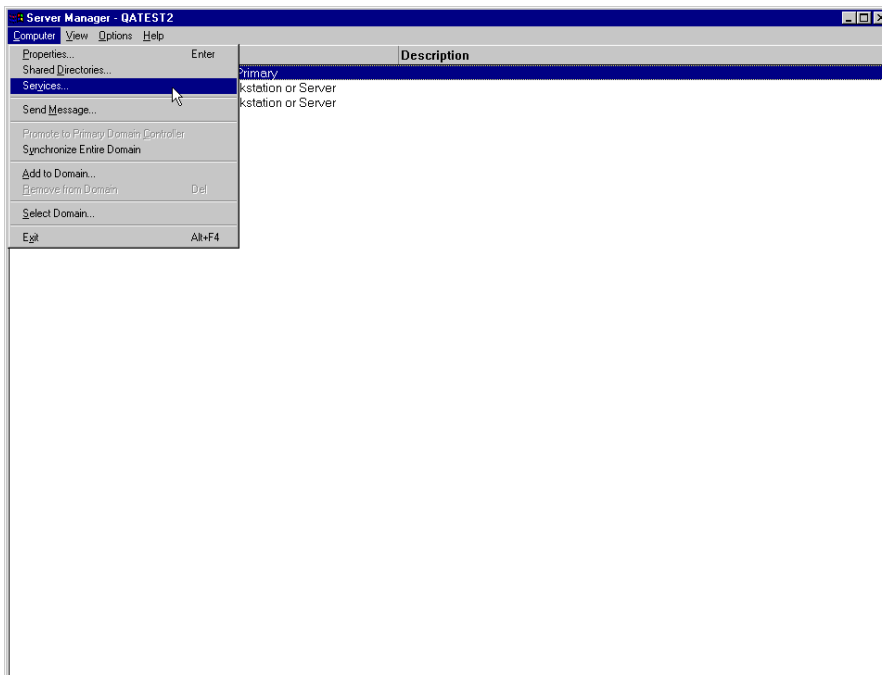
To Install RADIUS Server On an NT box.

Below we have used a simple RADIUS implementation to demonstrate Steel-Belted RADIUS from Funk software integrated with SonicWALL VPN solution. An evaluation version of Steel-Belted RADIUS Software is available from [www.funk.com](http://www.funk.com). For more information regarding other RADIUS Server brands compatibility, please refer to SonicWALL website.

After installing the Radius Server on a NT box, start the Radius Server Service on NT box from the Server Manager. Starting the Server Manager on NT is shown below.



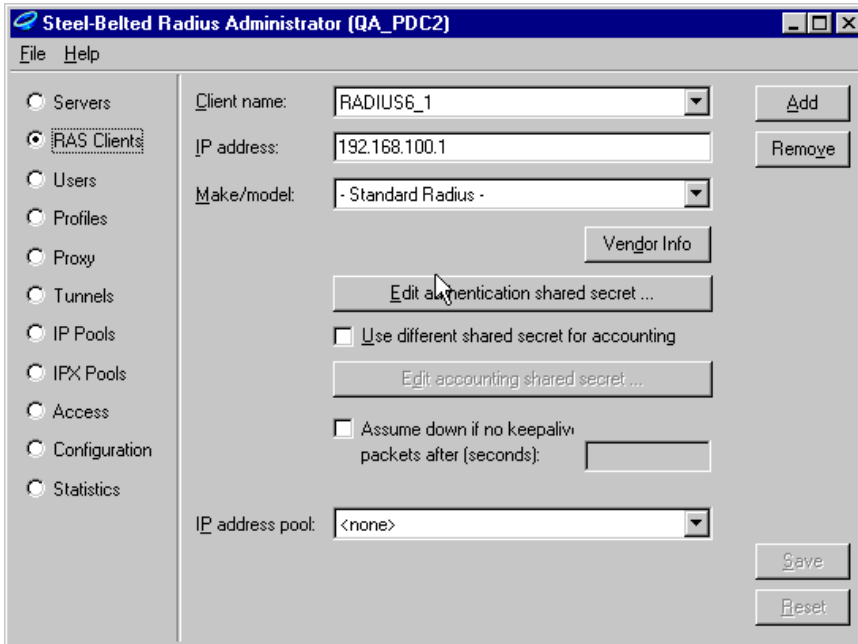
Select services from the File menu as shown below and select RADIUS. Start the service if not already started.



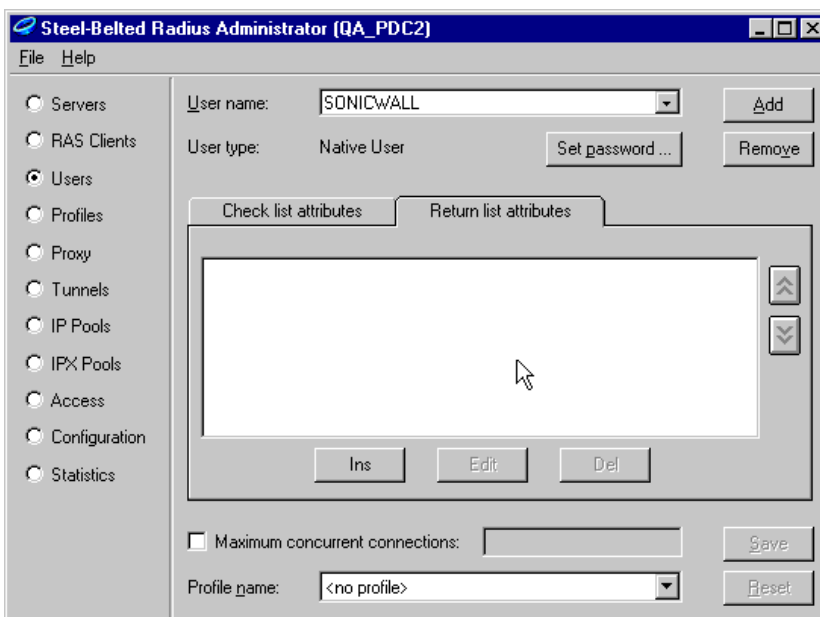
After starting the Server Manager, start the RADIUS Administrator Screen from the Start Menu



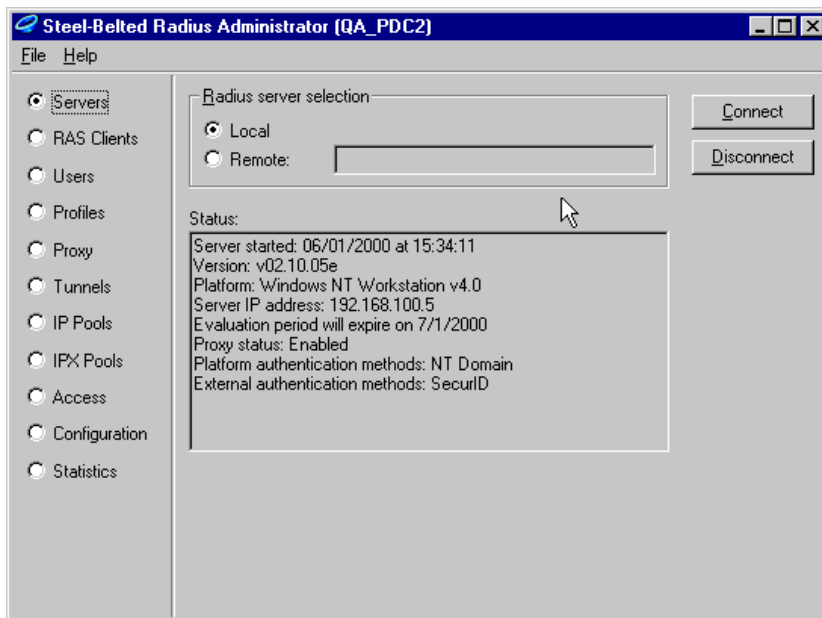
Configure the IP address of the RADIUS Server (SonicWALL LAN IP) and assign a Client Name with shared secret



Enter user names and passwords of persons with VPN client access.



Connect the RADIUS server by selecting **Local** and pressing the **Connect** button.



### **RSA ACE Server Configuration for SecurID®**

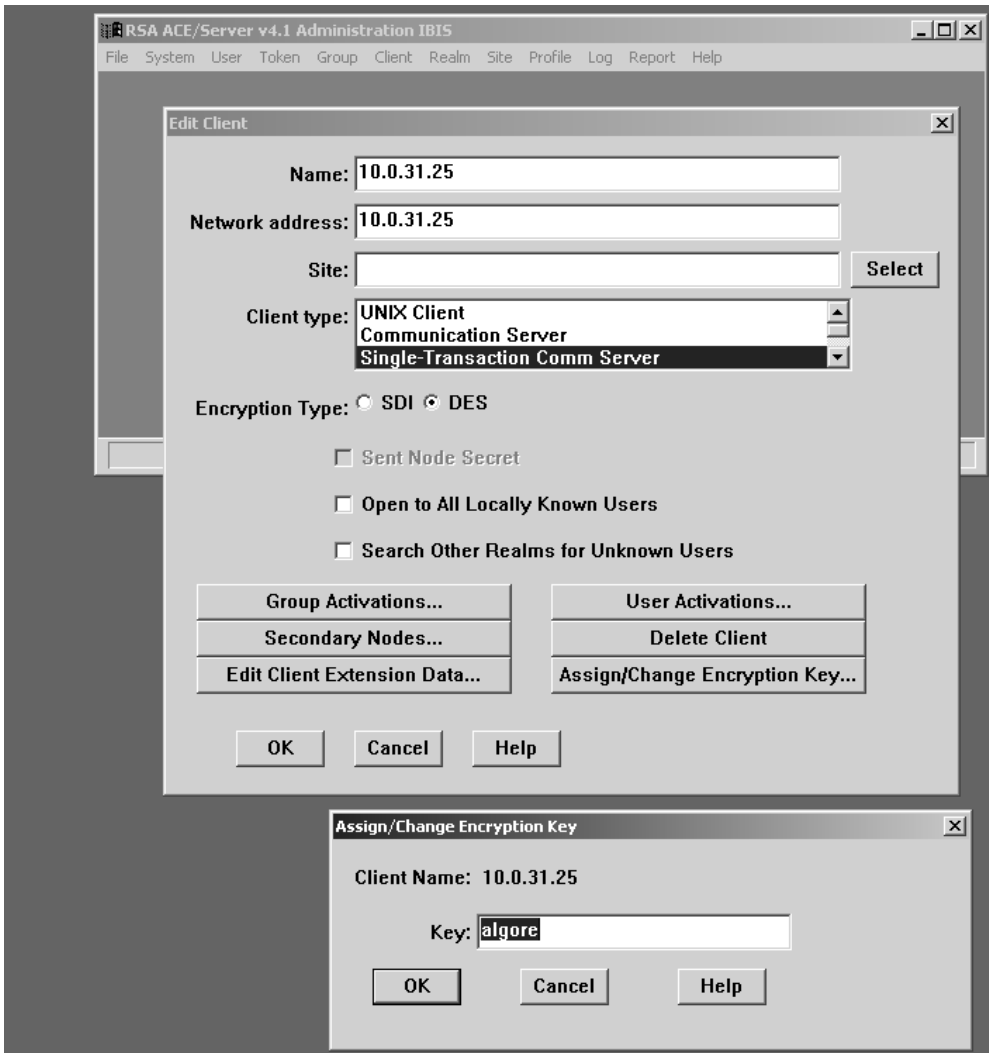
It is assumed that general ACE server concepts are understood.

Before proceeding, check that your ACE Server has RADIUS enabled. The SonicWALL will act as a **RADIUS** client when communicating with the ACE server.

First, configure the ACE server to accept authentication requests from the SonicWALL acting as a RADIUS Client. Add a Client from under the Client menu on the ACE Server GUI as shown below.

While configuring the ACE server, please configure both the SonicWALL RADIUS client and the ACE Server to use the same port numbers.

If, after adding a new RADIUS client, you do not see the **Assign Change Encryption Key** button enabled as shown below, please save and close **the Edit Client** screen. Then reopen it.

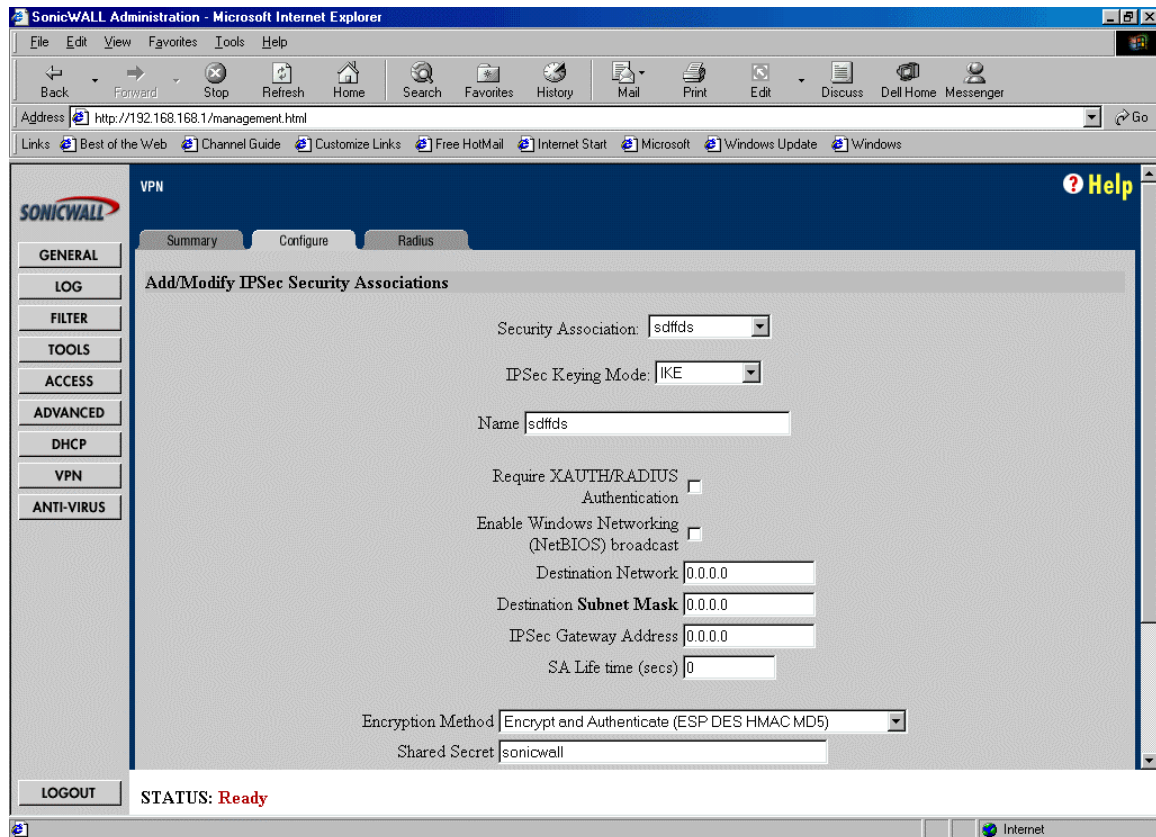


## To Configure VPN Security Association to Enforce RADIUS/ACE server VPN Client Authentication

Configure a GROUP VPN Tunnel on the SonicWALL as Shown below and enable RADIUS.

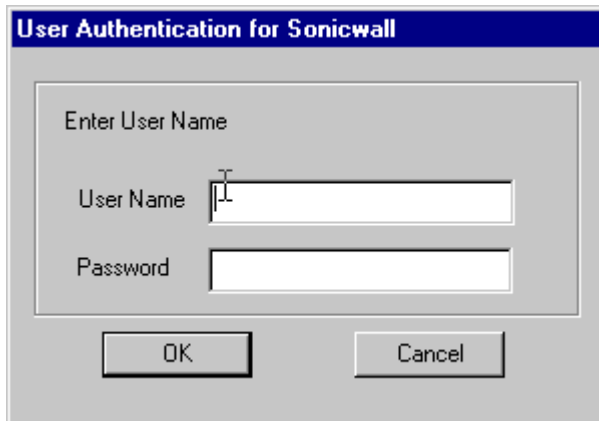
**Note:** RADIUS only works with VPN Client to Box tunnels

Below is a screen shot from firmware version 5.0



Configure the SonicWALL VPN client as described in the manual

When a remote VPN client user tries to access the private protected LAN through an SA requiring RADIUS/XAUTH, the VPN client automatically prompts the user for a User Name and Password.



If the user enters the correct RADIUS password, the user is automatically connected to the protected LAN.

If using RSA SecurID, enter the corresponding ACE username and password+pin into the VPN client XAUTH username/password prompt.

However, if a user enters the incorrect information, the following screen appears:

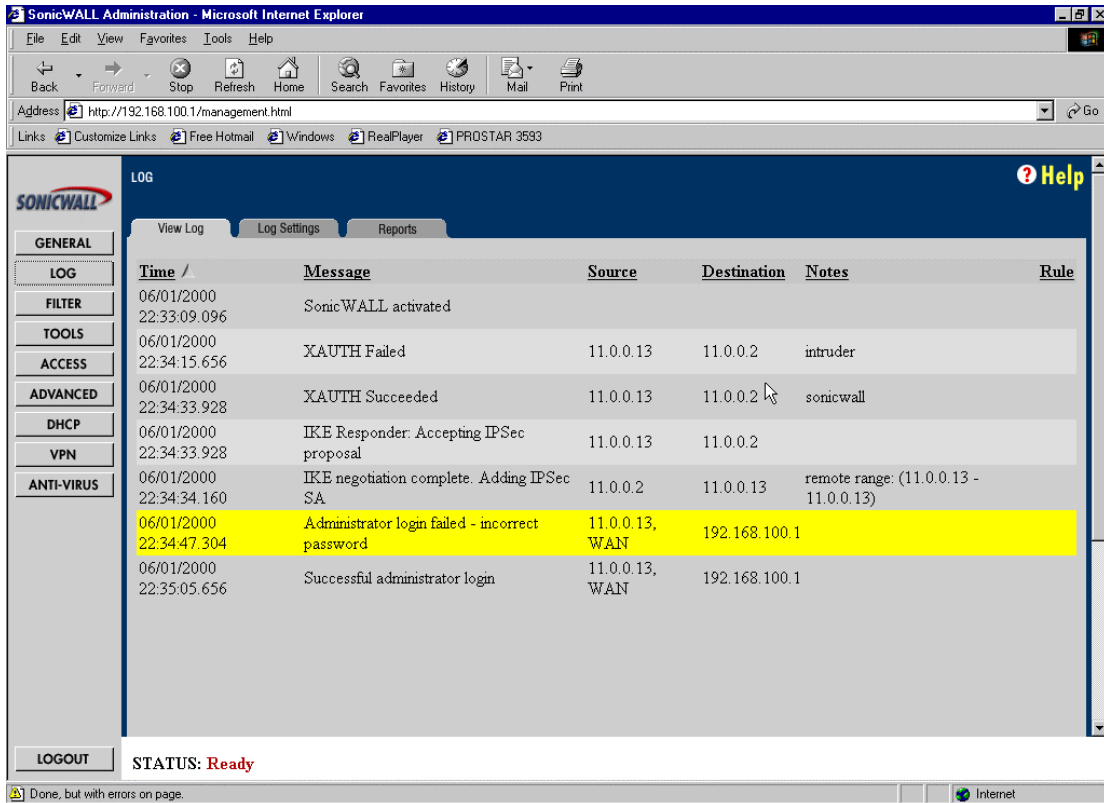


**Trouble Shooting Tip:**

If a VPN Client user enters the correct RADIUS username and password, but still sees the above **User Authentication Failed** screen, verify that the RADIUS server is up. From the LAN, ping the host NT box, verify that the RADIUS service is running, and the Server is connected.

**LOGGING OPTIONS AND CLIENT LOGON NOTIFICATION**

The SonicWALL log shows successful and failed User logon using XAUTH/RADIUS and displays the IKE negotiation of the VPN tunnel as shown below.



The VPN client also displays extra information in the log when XAUTH is used. Below is a screen shot of the VPN client log with successful XAUTH/RADIUS authentication and VPN tunnel negotiation indicated by the SPI values on the bottom line.

