RSA SecurID Ready Implementation Guide

Last Modified: January 25, 2006

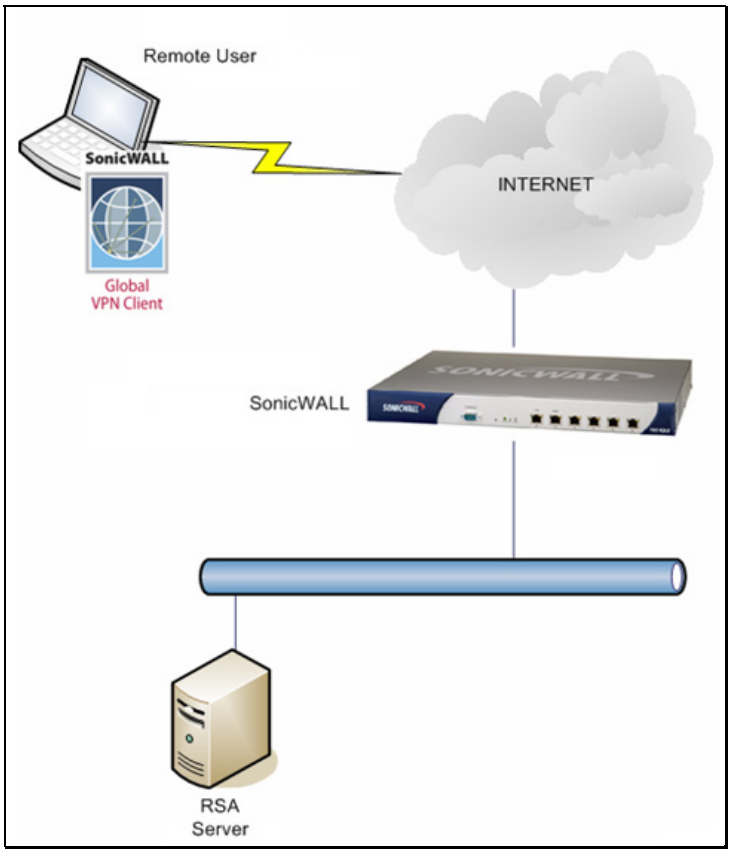
Partner Information

Product Information	
Partner Name	SonicWALL Inc.
Web Site	www.sonicwall.com
Product Name	SonicWALL TZ & PRO Products
Version & Platform	SonicOS Enhanced 3.1.0.12
Product Description	SonicWALL TZ and PRO Unified Threat Management Firewalls integrate advanced security services for true multi-layered security, including Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, Complete Anti-Virus and Content Filtering Service all manageable by SonicWALL's award-winning Global Management System. SonicOS Enhanced security operating system includes a streamlined Web GUI and comprehensive suite of easy-to-use configuration and management wizards that guide users through the configuration steps for common user network environments or scenarios, making it simple to set up in any network environment. SonicOS Enhanced supports RSA SecurID authentication via the RADIUS protocol.
Product Category	Perimeter Defense (Firewalls, VPNs & Intrusion Detection)

Solution Summary

SonicWALL TZ and PRO products running SonicOS Enhanced enable two-factor authentication for secure remote and wireless access utilizing SonicWALL Global VPN Client and RSA SecurID solutions.

Partner Integration Overview	
Authentication Methods Supported	RADIUS
List Library Version Used	5.0.3
RSA Authentication Manager Name Locking	N/A
RSA Authentication Manager Replica Support	N/A
Secondary RADIUS Server Support	Yes. Primary/Secondary RADIUS servers
Location of Node Secret on Agent	In flash
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	Designated Users, All Users, Default Method
RSA SecurID Protection of Administrative Users	No
RSA Software Token API Integration	No
Use of Cached Domain Credentials	No



Product Requirements

Partner Product Requirements: SonicWALL TZ & PRO Products	
TZ Family	TZ 170, TZ 170 SP, TZ 170 SPW, TZ 170 W
PRO Family	PRO 1260, PRO 2040, PRO 3060 PRO 4060, PRO 4100, PRO 5060
Firmware Version	SonicOS Enhanced 3.1.0.12
Additional Software Requirements	
SonicWALL Global VPN Client	3.1.0.556

Partner Product Requirements: SonicWALL Global VPN Client	
CPU	Intel x86 Compatible
Memory	32MB (Windows 98 SE/Me)
	64MB (Windows NT 4.0)
	128MB (Windows 2000/XP Home/Professional)
Storage	38MB

Operating System	
Platform	**Required Patches**
Microsoft Windows 98 SE/Me	All patch levels supported
Microsoft Windows NT 4.0	Service Pack 6.0 or greater
Microsoft Windows 2000 Professional	Service Pack 3.0 or greater
Microsoft Windows XP Home/Professional	All patch levels supported

Agent Host Configuration

To facilitate communication between SonicOS Enhanced and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the SonicWALL within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces
- RADIUS Secret (When using RADIUS Authentication Protocol)

When adding the Agent Host Record, you should configure the SonicWALL as a Communication Server. This setting is used by the RSA Authentication Manager to determine how communication with SonicOS Enhanced will occur.

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host records.

Partner Authentication Agent Configuration

Before You Begin

This section provides instructions for integrating the partners' product with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Documenting the Solution

SonicWALL TZ and PRO products running SonicOS Enhanced support secure two-factor authentication for Global VPN Client tunnels via the RADIUS protocol. The following configuration steps must be preformed in order implement this solution.

On the SonicWALL security appliance:

- Set up the User's Authentication Method
- Create new GroupVPN Policy for the Global VPN Client
- Verify that applications function properly through the tunnel

On the computer requiring secure remote access via SonicWALL Global VPN Client:

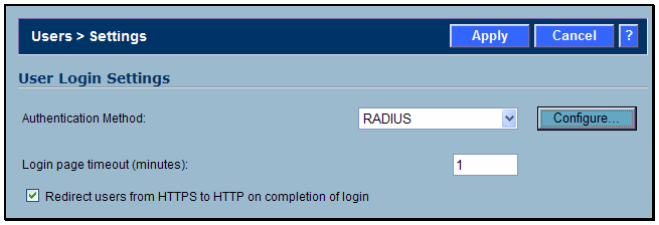
- Install SonicWALL Global VPN Client
- Create a Profile for Connecting to the SonicWALL security appliance

SonicOS Enhanced Configuration

SonicWALL recommends that customers update to the latest version of SonicOS Enhanced prior to completing this configuration.

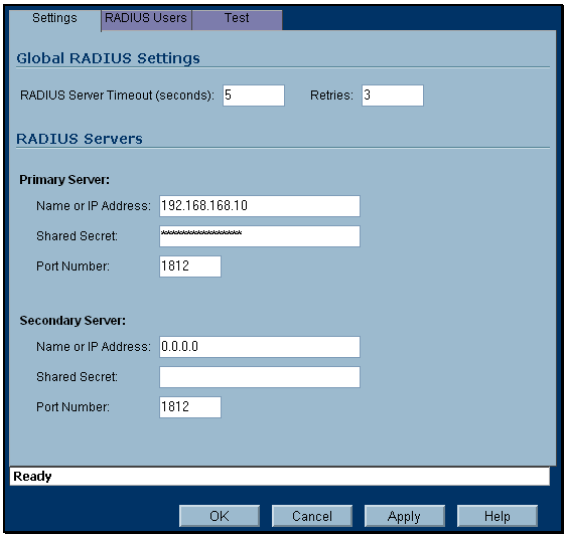
Configuring RADIUS

1. In **Users > Settings** under **User Login Settings**, set the Authentication Method to **RADIUS** from the drop-down menu, and click the **Configure** button.

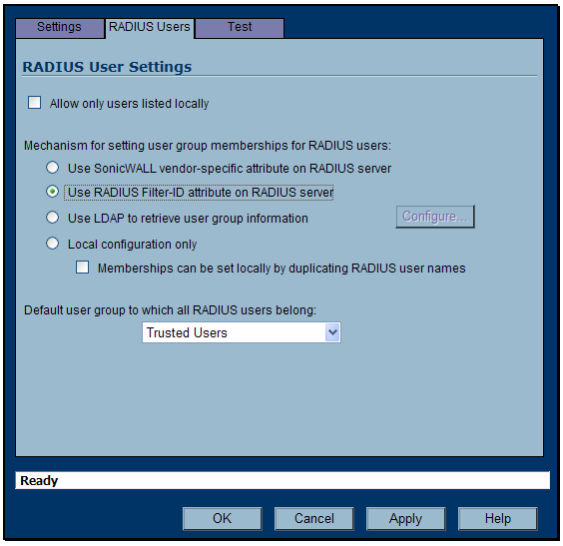


Note: After the RADIUS authentication method is enabled the SonicWALL security appliance can only be accessed using HTTPS Management.

2. In the **Primary Server: Name or IP Address** field, enter the RSA Authentication Manager Servers IP Address.
3. Create a **Shared Secret** to authenticate the SonicWALL to the RSA Authentication Manager Server. This same secret will be used when you create the Agent Host records in the RSA Authentication Manager Server configuration.
4. Set the **Port Number** to 1812.



5. Select the **RADIUS Users** tab, and select the **Use Radius Filter-ID attribute on Radius Server**.
6. Select **Trusted User** from the drop-down box under **Default user group to which all RADIUS users belong**.

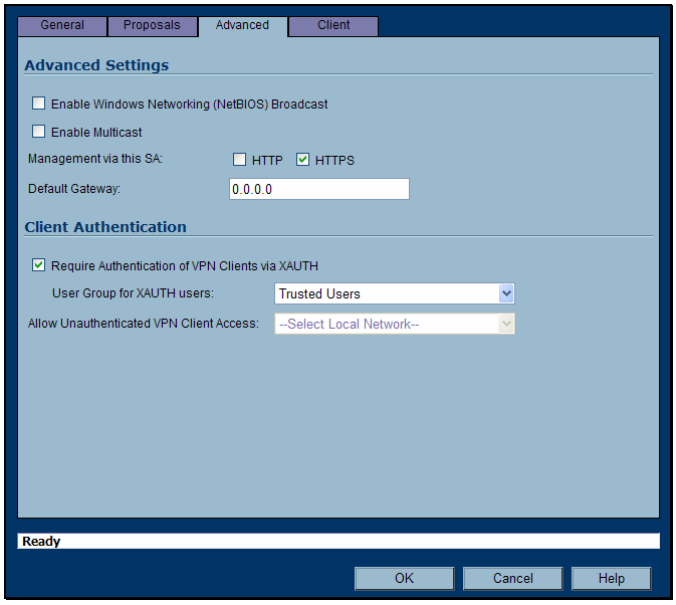


7. Click **OK**.

Note: The RADIUS Testing tool may not work due to encryption type mismatches. Please use the RSA Log Monitor application for testing and debugging purposes.

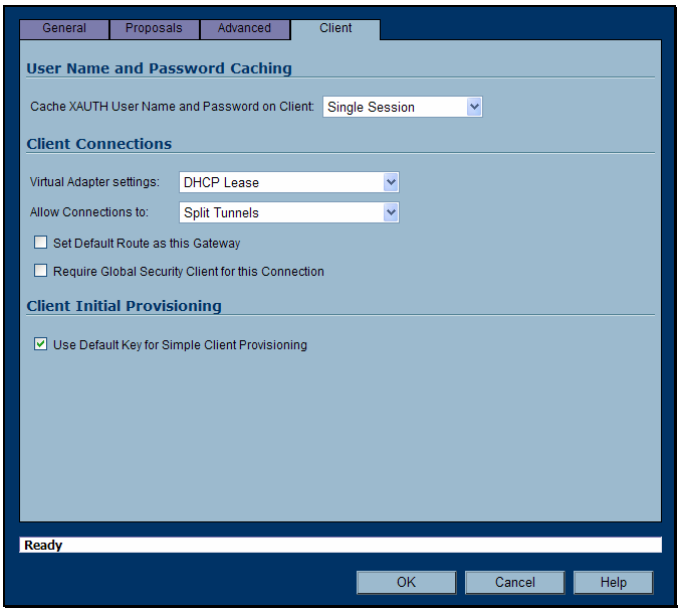
Configuring Global VPN Client Settings

8. In **VPN > Settings**, click the **Configure** icon for the **WAN GroupVPN**, and select the **Advanced** Tab.
9. Select **Require Authentication of VPN Clients via XAUTH**, and select the **Trusted Users** group as the **User Group for XAUTH users**.



10. Select the **Client** Tab, and set the following parameters:

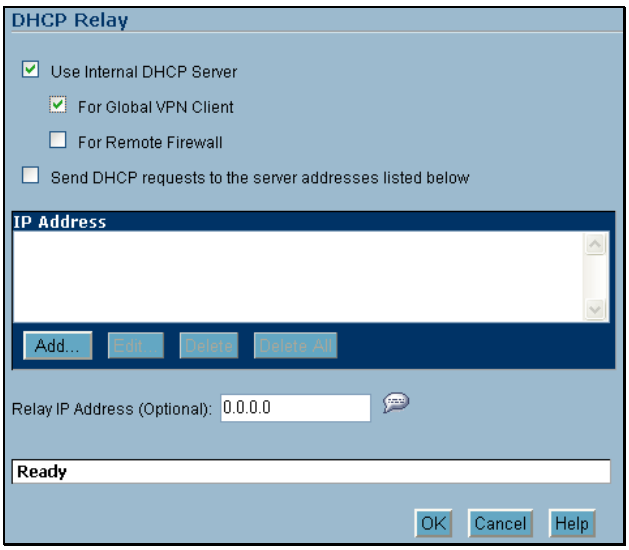
    - Set **Cache XAUTH User Name and Password on Client** to **Single Session**.
    - Set **Virtual Adapter settings** to **DHCP Lease** (or **DHCP Lease or Manual Config** if you wish to statically address the virtual adapter).
    - Select the **Use Default Key for Simple Client Provisioning** checkbox.



11. Click **OK**.

Configuring DHCP over VPN

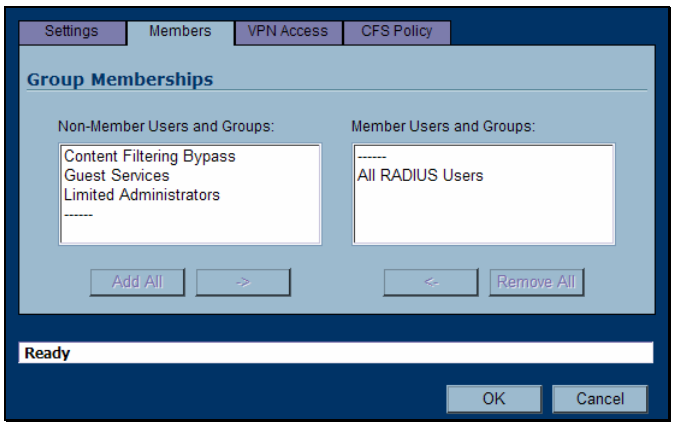
12. Select **VPN > DHCP over VPN** and click the **Configure** icon for Central Gateway.
13. Select the **Use Internal DHCP Server** and **For Global VPN Client** check boxes.



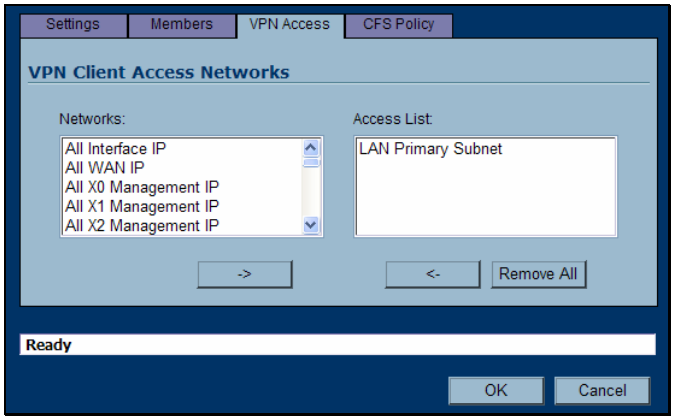
14. Click **OK**.

Configuring User Group Settings

15. Select **Users > Local Groups** and click the **Configure** icon for Trusted Users.
16. Select the **Members' tab**, and confirm **All RADIUS Users** is in the **Members Users and Groups**.



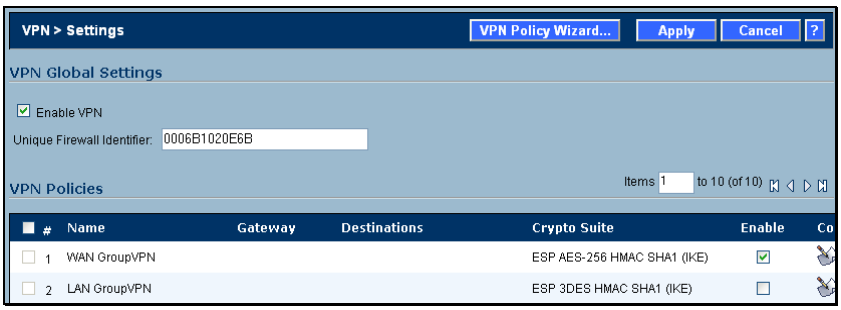
17. Select **VPN Access** tab, and add the LAN Primary Subnet.



18. Click **OK**.

Enable Global VPN Client Connections

19. Select **VPN > Settings**.
20. Select the **Enable VPN** checkbox.
21. Select the **Enable** checkbox for the **WAN GroupVPN** policy.



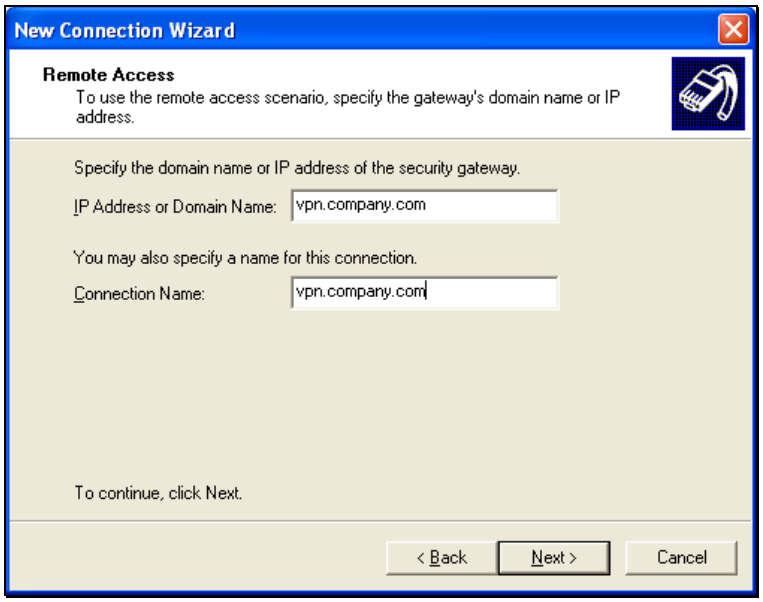
SonicWALL Global VPN Client Configuration

Download and install the SonicWALL Global VPN Client by logging in to your mySonicWALL account at **www.mysonicwall.com**. Once installed, simply use the New Connection Wizard to create a connection to your SonicWALL as detailed below.

22. Create a new VPN Connection using the New Connection Wizard. Select the **File > New Connection item** to launch the wizard. Click **Next** to continue to the next screen of the wizard.

23. Select the **Remote Access** radio button and click the **Next** button.

24. Enter the WAN IP Address or the DNS address of the SonicWALL that you are going to connect to. Click the **Next** button when finished.



25. Click the **Finish** button to complete the wizard.

Certification Checklist

Date Tested: December 19, 2005

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.0	Windows XP Service Pack 2
SonicWALL Pro 2040	3.1.0.12	SonicOS Enhanced
SonicWALL GlobalVPN Client	3.1.0.556	Windows XP Service Pack 2

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	N/A	Force Authentication After New PIN	✓
System Generated PIN	N/A	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	N/A	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	N/A	User Defined (5-7 Numeric)	✓
User Selectable	N/A	User Selectable	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
PASSCODE			
16 Digit PASSCODE	N/A	16 Digit PASSCODE	✓
4 Digit Password	N/A	4 Digit Password	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
Name Locking Enabled	N/A	Name Locking Enabled	
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓

Additional Functionality			
RSA Software Token API Functionality			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
Domain Credential Functionality			
Determine Cached Credential State	N/A	Determine Cached Credential State	
Set Domain Credential	N/A	Set Domain Credential	
Retrieve Domain Credential	N/A	Retrieve Domain Credential	

BSD / SNW

✓ = Pass ✗ = Fail N/A = Non-Available Function

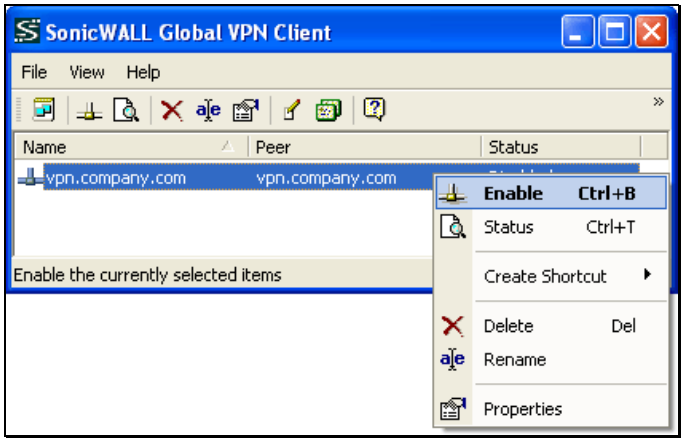
Appendix

GlobalVPN Client Authentication Example with RSA SecurID

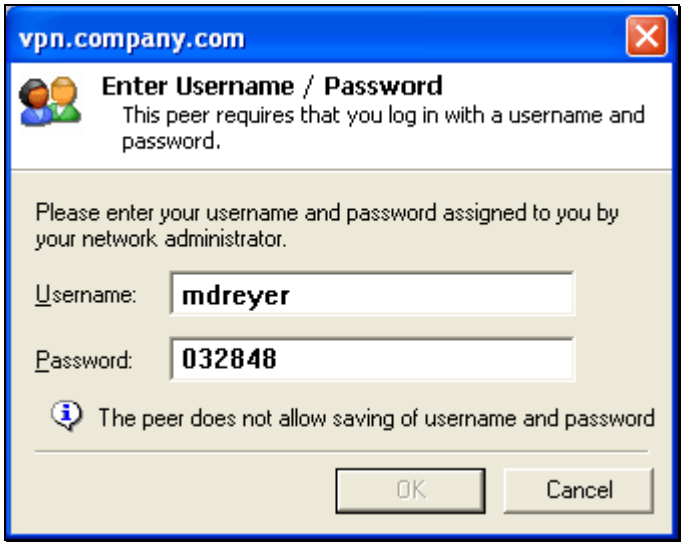
New user GlobalVPN Client login process overview:

- Enable the GVC VPN Connection
- Authenticate with username and tokencode
- Allow the system to generate a new PIN
- Agree to the system generated PIN
- Accept the new PIN by entering the next tokencode
- Authenticate with username and PASSCODE (PIN + tokencode)

26. Right click on the VPN Connection and select **Enable** from the popup menu.



27. Authenticate with username and tokencode. In the Password field enter the series of numbers displayed on the token. Click **OK** to begin the authentication process.



28. Enter **y** and click **OK** to generate a new PIN.

29. Accept the new PIN by entering **y** and clicking **OK**.

30. Wait for the tokencode to change, enter the PASSCODE and Click **OK.**

31. The VPN Connection will now be established. In the future the user will only be required to enter the PIN and tokencode (PASSCODE) in order to authenticate.