

Funk Software AdmitOne VPN Client to SonicWALL Configuration

Prepared by SonicWALL, Inc.

September 2002

The following document details the configuration settings for the Funk Software AdmitOne VPN Client that enables Pocket PCs to terminate VPN connections to SonicWALL Internet Security Appliances with version 6.3.1.0 firmware.

Now with Funk Software AdmitOne VPN Client, your mobile users can now safely work from home or other remote locations and securely access the company's network and internal resources.

SonicWALL Configuration Settings

The Pocket PC should be treated like a Dynamic IP Site-to-Site IKE VPN tunnel from the SonicWALL's perspective.

VPN SA Name = AdmitOne VPN Client UserName
IKE PreShared Key = PreShared Key defined in the AdmitOne client
Remote IPsec Gateway = 0.0.0.0
IKE Encryption Scheme = 3DES or DES
IKE Authentication Scheme = SHA-1 or MD5
IPSEC Encryption Scheme = 3DES or DES
IPSEC Authentication Scheme = SHA-1 or MD5
Phase 1 DH Group = 1, 2 or 5
VPN Destination Network = any size subnet, except for /32 (smallest is /31 - 2 IP Addresses),
The AdmitOne VPN Client software will use this as the Client IP Pool Subnet.

The screenshot shows the SonicWALL VPN configuration interface. At the top, there is a 'VPN' header with a 'Help' icon. Below the header are tabs for 'Summary', 'Configure', 'Authentication Service', 'Local Certificates', and 'CA Certificates'. The main content area is titled 'Add/Modify IPsec Security Associations'. It contains several fields: 'Security Association' (dropdown menu with 'Test' selected), 'IPsec Keying Mode' (dropdown menu with 'IKE using Preshared Secret' selected), 'Name' (text input field with 'Test'), 'Disable This SA' (checkbox, unchecked), and 'IPsec Gateway Address' (text input field with '0.0.0.0'). Below this is a section titled 'Security policy' with fields for 'Phase 1 DH Group' (dropdown menu with 'Group 1' selected), 'SA Life time (secs)' (text input field with '28800'), 'Phase 1 Encryption/Authentication' (dropdown menu with '3DES & MD5' selected), 'Phase 2 Encryption/Authentication' (dropdown menu with 'Strong Encrypt and Authenticate (ESP 3DES HMAC MD5)' selected), and 'Shared Secret' (text input field with 'admitone').

Figure 1 SonicWALL VPN Configuration

Page 1 of 2

AdmitOne VPN Client Configuration

This assumes that the AdmitOne Client software has been successfully installed on the Pocket PC.

The "Security Policy Store" is secured by a local username and password - you must configure one and it must be entered when the AdmitOne VPN Client software is launched.

1. On the main Window, go to "Secure Connections" and double-click "New Connections". Enter a "Name" for the VPN Connection – example "Access to Corporate Network"
2. Enter the IP Address for the VPN Gateway in the "Tunnel Gateway IP Address"
3. Uncheck the box labeled "Use IP Address as Identity" - since the SonicWALL SA is setup with a Dynamic IP Gateway, it expects a FQDN (Fully Qualified Domain Name) IKE ID and not IP_ADDR IKE ID
4. Enter the SNWL VPN SA Name in the "User's Identity" field
5. Enter the PreShared Key in the "Shared Secret" field
6. Uncheck the box labeled "Auto IPsec/IKE Setup" (SNWL does not currently support Quick Mode)
7. On the bottom left side of the screen, you will see an "Advanced" Menu option. Select this to configure the IKE and IPsec settings.
 - a. IKE Settings - Encryption Algorithm, Hash Algorithm, Diffie Hellman Group and PFS options
 - b. PFS must match the one used in Phase 1
 - c. IPsec Settings - Encryption Algorithm, Hash Algorithm and "Enable NAT Traversal" options
 - d. Uncheck the compression feature.
 - e. Uncheck "Enable NAT Traversal" (There are 3 different IETF drafts available, no consensus yet)
8. Select "Next" to continue VPN Setup
9. Check the box labeled "Enable Virtual Adapter" - this is how the SonicWALL will recognize the PDA Client
 - a. Enter an IP Address in the IP Address Field
 - b. Enter a Subnet Mask in the Subnet Mask Field (the smallest subnet mask is /31. One IP is used for the PDA and the other IP is used for the PDA's virtual default gateway)
10. Select "Next" to continue VPN Setup
11. Use the "Specified IP Address Ranges" option and specify the IP Subnets that are accessible through the VPN tunnel
12. Select "Finish" to complete the VPN Configuration

Connecting with the AdmitOne VPN Client

Select the VPN Profile you wish to connect to and press the "Connect" button. Use the adapter's ping utility to test the VPN connection. If the adapter does not have a Ping utility, then it is recommended to use the Internet Explorer to test the connection.

Other Notes:

- Admit-One VPN Client will propose Phase 1 and Phase 2 Lifetime to be 3600 Seconds
- Admin-One VPN Client will re-propose VPN Negotiations at 50% of the current lifetime
- NAT-Traversal Detection and Support is not compatible
- XAUTH will be supported in the next version of the client

The AdmitOne VPN Client is completely configurable, but the majority of settings have been hidden from interface. For more information on customizing the AdmitOne Client software, please see the AdmitOne Installation Manual.

Since the Pocket PC is the dynamic IP mode, it will be responsible for bringing up the VPN tunnel. Renegotiation for VPN tunnels occurs in 1-2 seconds, so it should not be noticeable.