

# Creating IKE IPSec VPN Tunnels between SonicWALL Devices and Cisco 3000 VPN Concentrators

*Prepared by SonicWALL, Inc.  
05/14/2002*

## Introduction

This technote will detail all the steps necessary to create a working IKE IPSec VPN tunnel between a SonicWALL device and a Cisco 3000 VPN Concentrator (formerly known as the Altiga VPN Concentrator). This technote assumes that both sides have static IP addresses for the external WAN interfaces. SonicWALL engineering has tested and validated the settings described in this technote. Please note that all settings and screenshots contained within this technote are taken from a SonicWALL TELE2 device running firmware 6.3.1.0, and a Cisco 3005 VPN Concentrator running firmware 3.5.1.0.

## Before You Begin

SonicWALL strongly recommends using firmware release 6.3.1.0 or newer on the SonicWALL device, and 3.5.0.0 or newer on the Cisco 3000 VPN Concentrator.

This was a problematic pairing until recent software releases for both hardware platforms; connectivity and renegotiation issues may occur if either side is not running the above-recommended software releases.

Using a long SA lifetime may reduce issues with SA's timing out and failing to renegotiate. The downside to doing this is that it's inherently less secure than using standard SA lifetimes like 28,800 seconds (8 hours) and 86,400 seconds (24 hours). For reference, the maximum lifetime for a Cisco 3000 VPN Concentrator SA is 2,147,483,647 seconds, and the maximum lifetime for a SonicWALL device SA is 9,999,999 seconds. Another drawback of this method is that if one side crashes or reboots during this SA lifetime, it may be necessary to restart the other side to clear out the invalid SA.

If the SonicWALL is the 'IKE Initiator', you will see this in the Cisco 3000 VPN Log: "Mismatch: Configured LAN-to-LAN proposal differs from negotiated proposal". This message can be ignored. Since the SonicWALL now has a user-selectable keepalive mechanism for SA's as of firmware 6.1.1.0, it will generally be the 'IKE Initiator'.

Most of the predefined IKE entries in the Cisco 3000 VPN use Diffie-Hellman 2 (DH2). Please take special care to correctly set the Diffie-Hellman (DH) group type on the SonicWALL device and the Cisco 3000 VPN. If the wrong defaults are used on both sides to set up a VPN tunnel, it may result in the ability to initiate a tunnel from the Cisco 3000 VPN to the SonicWALL device, yet be unable to initiate a tunnel from the SonicWALL device to the Cisco 3000 VPN.

By default, the Cisco 3000 VPN Concentrator will use 86,400 seconds for 'IKE' and the 'L2L IPSec SA' lifetimes and is customizable for both phases, but the SonicWALL device will use 28,800 seconds by default for both SA lifetimes (you can't set different lifetimes for the two phases). This disparity in the lifetimes will cause problems if not changed to match on both sides.

**SonicWALL Setup**

1. Log into the SonicWALL's Management GUI using a current web browser, such as Microsoft IE 5.5 or Netscape 6.2.
2. Click on the 'VPN' button on the left side, and then click on the 'Configure' tab along the top.
3. From the 'Security Association' drop-down box, choose "-Add New SA-".
4. From the 'IPSec Keying Mode' drop-down box, choose "IKE using Preshared Secret".
5. In the 'Name' field, enter a unique name for your tunnel to the Cisco VPN Concentrator.
6. In the 'IPSec Gateway Address' field, enter the static IP address of the 'Public' interface of the Cisco 3000 VPN Concentrator.
7. From the 'Phase 1 DH Group' drop-down box, choose "Group 1".
8. In the 'SA Life time (secs)' field, enter in the security association lifetime in seconds you wish to use for the VPN tunnel to the Cisco 3000 VPN Concentrator.
9. From the 'Phase 1 Encryption/Authentication' drop-down box, choose "3DES & MD5".
10. From the 'Phase 2 Encryption/Authentication' drop-down box, choose "Strong Encrypt and Authenticate (ESP 3DES HMAC MD5)".
11. In the 'Shared Secret' field, enter in the shared secret you wish to use for the VPN tunnel to the Cisco 3000 VPN Concentrator.
12. Choose the 'Specify Destination Networks Below' radio button.
13. Click on the 'Add New Network...' button.
14. In the pop-up screen that appears, enter in the subnet and mask that are behind the 'Private' interface of the Cisco 3000 VPN Concentrator (you may need to use the 'Add New Network..' button multiple times if there are multiple subnets) and then click on the 'Update' button when you are done.
15. Click on the 'Advanced Settings...' button.
16. In the pop-up screen that appears, check the 'Enable Keep Alive' box and then click on the 'OK' button when you are done.
17. Click on the 'Update' button in the lower-right-hand of the screen to save all changes.

## Creating IKE IPSec VPN Tunnels between SonicWALL Devices and Cisco 3000 VPN Concentrators

## SonicWALL Device Screenshots

Sample of IPSec Security Association to Cisco 3000 VPN Concentrator (top half):

The screenshot displays the SonicWALL Administration web interface in Microsoft Internet Explorer. The browser's address bar shows the URL `https://192.168.76.1/management.html`. The interface features a navigation menu on the left with categories like General, Log, Filter, Tools, Access, Advanced, DHCP, VPN, Anti-Virus, and High Availability. The main content area is titled "Add/Modify IPSec Security Associations" and includes the following configuration fields:

- Security Association: `cisco3005`
- IPSec Keying Mode: `IKE using Preshared Secret`
- Name: `cisco3005`
- Disable This SA:
- IPSec Gateway Address: `65.70.200.60`

Under the "Security policy" section, the configuration includes:

- Phase 1 DH Group: `Group 1`
- SA Life time (secs): `86400`
- Phase 1 Encryption/Authentication: `3DES & MD5`
- Phase 2 Encryption/Authentication: `Strong Encrypt and Authenticate (ESP 3DES HMAC MD5)`
- Shared Secret: `4k#Tama49`

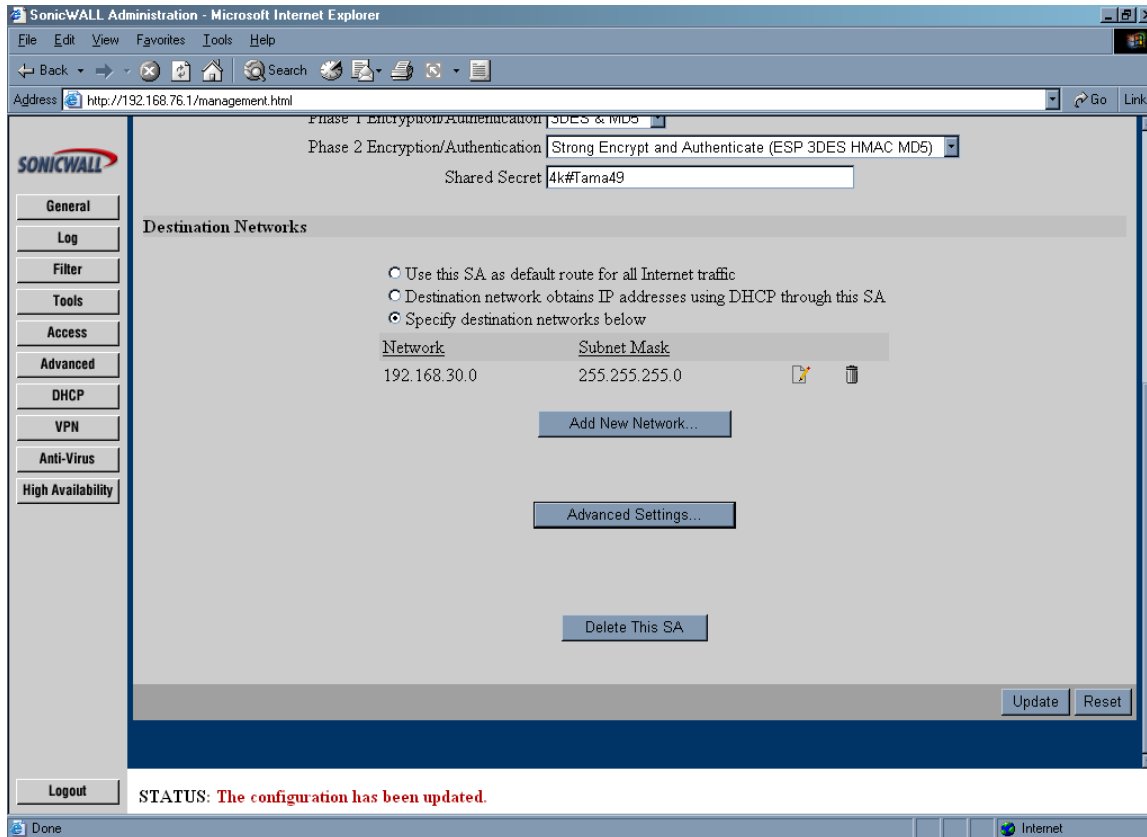
The "Destination Networks" section contains three radio button options:

- Use this SA as default route for all Internet traffic
- Destination network obtains IP addresses using DHCP through this SA
- Specify destination networks below

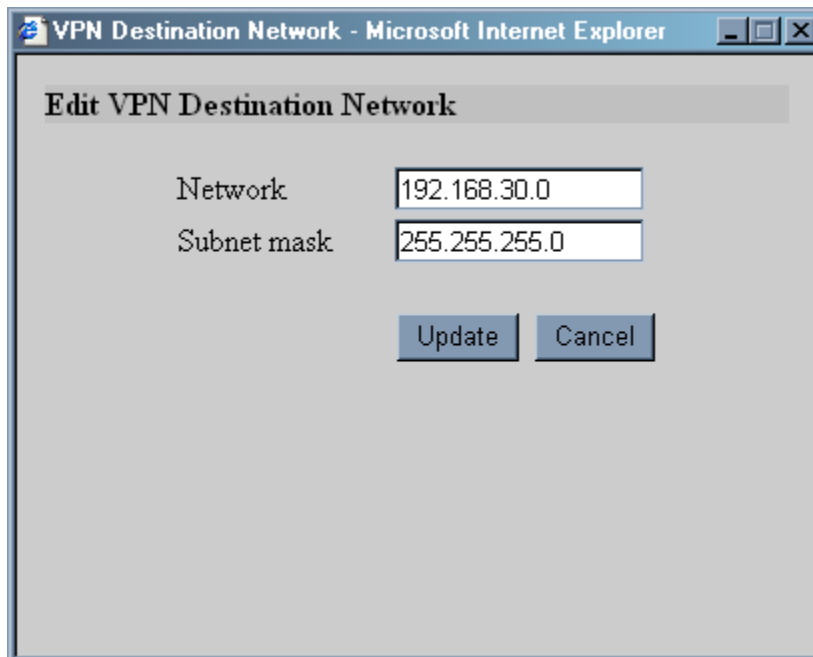
At the bottom of the configuration area, a status message reads: **STATUS: The configuration has been updated.**

Creating IKE IPSec VPN Tunnels between SonicWALL Devices and Cisco 3000 VPN Concentrators

Sample of IPSec Security Association to Cisco 3000 VPN Concentrator (bottom half):



Sample of 'Add New Network':



Sample of 'Advanced Settings':

VPN Advanced Settings - Microsoft Internet Explorer

### Edit Advanced Settings

Use Aggressive Mode

Enable Keep Alive

Require authentication of local users

Require authentication of remote users

Remote users behind VPN gateway

Remote VPN clients with XAUTH

Enable Windows Networking (NetBIOS) broadcast

Apply NAT and firewall rules

Forward packets to remote VPNs

Enable Perfect Forward Secrecy


Phase 2 DH Group

Default LAN Gateway

OK Cancel

*Note that after clicking OK you must click Update on the main page to save changes made here.*

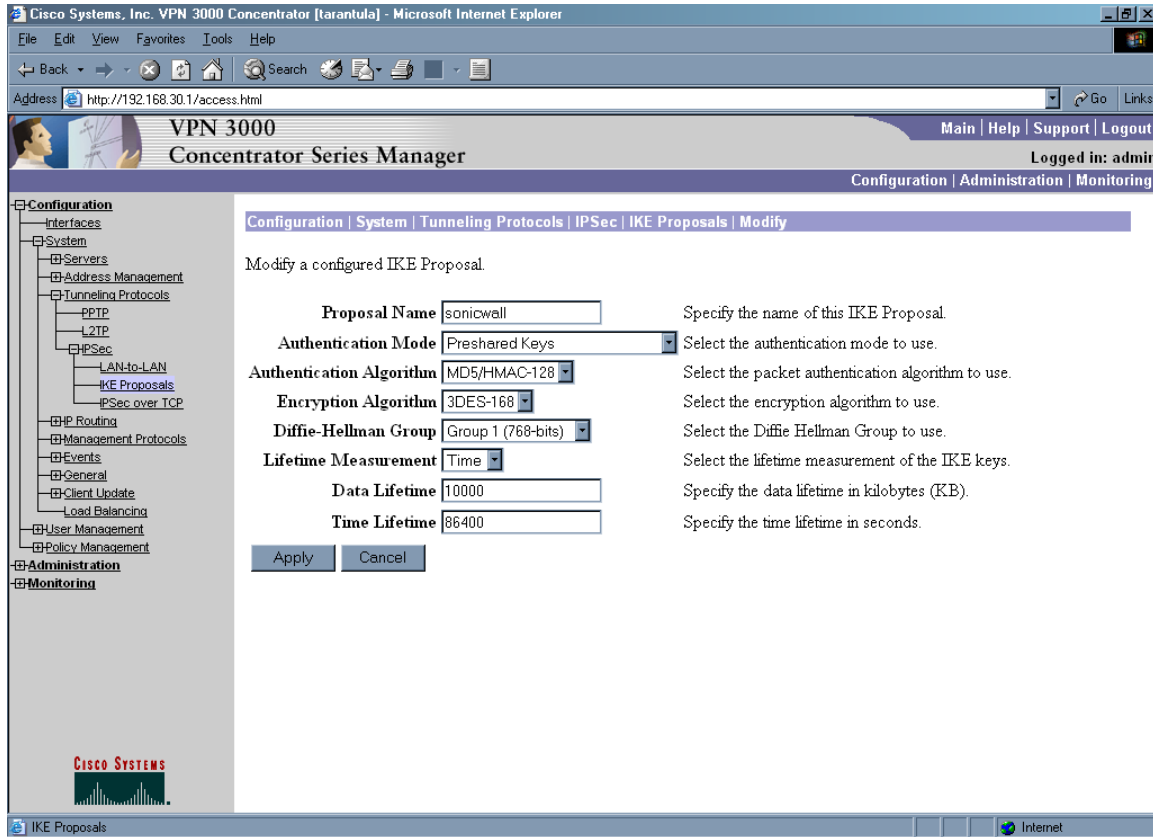
**Cisco 3000 VPN Concentrator Setup**

1. Log into the Cisco 3000 VPN Concentrator's Management GUI using a current web browser, such as Microsoft IE 5.5 or Netscape 6.2.
2. Navigate to the 'Configuration/System/Tunneling Protocols/IPSec/IKE Proposals' section.
3. Click on the 'Add' button.
4. In the 'Proposal Name' field, enter in "sonicwall".
5. From the 'Authentication Mode' drop-down box, choose "Preshared Keys".
6. From the 'Authentication Algorithm' drop-down box, choose "MD5/HMAC-128".
7. From the 'Encryption Algorithm' drop-down box, choose "3DES-168".
8. From the 'Diffie-Hellman Group' drop-down box, choose "Group 1 (768-bits)".
9. From the 'Lifetime Measurement' drop-down box, choose "time".
10. In the 'Time Lifetime' field, enter in enter in the security association lifetime in seconds you wish to use for the VPN tunnel to the SonicWALL device.
11. Click on the 'Add' button.
12. Choose this new "sonicwall" proposal you've just created from the 'Inactive Proposals' section, and then click on the '<<Activate' button to move it to the 'Active Proposals' section.
13. Navigate to the 'Configuration/System/Tunneling Protocols/IPSec/LAN-to-LAN' section.
14. Click on the 'Add' button.
15. In the 'Name' field, enter in a unique name for your tunnel to the SonicWALL device.
16. From the 'Interface' drop-down box, choose the 'Public' interface.
17. In the 'Peer' field, enter in enter the static IP address of the 'WAN' interface of the SonicWALL device.
18. From the 'Digital Certificate' drop-down box, choose "None (Use Preshared Keys)".
19. In the 'Preshared Key' field, enter in the shared secret you wish to use for the VPN tunnel to the SonicWALL device.
20. From the 'Authentication' drop-down box, choose "ESP/MD5/HMAC-128".
21. From the 'Encryption' drop-down box, choose "3DES-168".
22. From the 'IKE Proposal' drop-down box, choose "sonicwall".
23. From the 'Routing' drop-down box, choose "None".
24. From the 'Local Network Network List' drop-down box, choose 'Use IP Address/Wildcard-mask below'; please note that if you have multiple subnets behind the 'Private' interface, you may first have to create a 'Network List' object from the 'Configuration/Policy Management/Traffic Management/Network Lists' section to use instead.
25. In the 'Local Network IP Address' field, enter in the subnet behind the 'Private' interface.
26. In the 'Local Network Wildcard mask' field, make sure the wildcard mask it auto-creates is correct, and adjust accordingly.
27. From the 'Remote Network Network List' drop-down box, choose 'Use IP Address/Wildcard-mask below'; please note that if you have multiple subnets behind the SonicWALL's 'LAN' interface, you may first have to create a 'Network List' object from the 'Configuration/Policy Management/Traffic Management/Network Lists' section to use instead.
28. In the 'Remote Network IP Address' field, enter in the IP subnet behind the SonicWALL's 'LAN' interface.
29. In the 'Remote Network Wildcard mask' field, make sure the wildcard mask it auto-creates is correct, and adjust accordingly.
30. Click on the 'Add' button.
31. At this point a confirmation screen will appear – click on the 'OK' button to create the VPN tunnel
32. Navigate to the 'Configuration/Policy Management/Traffic Management/SAs' section.
33. Select the IPSec SA to the SonicWALL Device (it will begin with "LTL:" and have the name you specified in step 4 above) and click on the 'Modify' button.
34. In the 'Time Lifetime' field, adjust the existing time to match the security lifetime you had specified above in step 10 above.
35. Click on the 'Apply' button to save the changes.
36. In the upper-right-hand corner of the screen, click on the 'Save Needed  link to save all changes to the startup configuration of the Cisco 3000 VPN Concentrator.

Creating IKE IPSec VPN Tunnels between SonicWALL Devices and Cisco 3000 VPN Concentrators

Cisco 3000 VPN Concentrator Screenshots

Sample of Custom IPSec IKE Proposal:



Creating IKE IPSec VPN Tunnels between SonicWALL Devices and Cisco 3000 VPN Concentrators

Sample of IPSec LAN-to-LAN Setup (top half):

The screenshot shows the configuration interface for an IPSec LAN-to-LAN connection on a Cisco VPN 3000 Concentrator. The browser window title is "Cisco Systems, Inc. VPN 3000 Concentrator [tarantula] - Microsoft Internet Explorer". The address bar shows "http://192.168.30.1/access.html". The page title is "VPN 3000 Concentrator Series Manager" and the user is logged in as "admin".

The configuration page is titled "Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Modify". The main heading is "Modify an IPSec LAN-to-LAN connection." The configuration fields are as follows:

- Name:** tosonicwall (Enter the name for this LAN-to-LAN connection.)
- Interface:** Ethernet 2 (Public) (65.70.200.60) (Select the interface to put this LAN-to-LAN connection on.)
- Peer:** 65.70.200.57 (Enter the IP address of the remote peer for this LAN-to-LAN connection.)
- Digital Certificate:** None (Use Preshared Keys) (Select the Digital Certificate to use.)
- Certificate:**  Entire certificate chain (Choose how to send the digital certificate to the IKE peer.)
- Transmission:**  Identity certificate only
- Preshared Key:** 4k#Tama49 (Enter the preshared key for this LAN-to-LAN connection.)
- Authentication:** ESP/MD5/HMAC-128 (Specify the packet authentication mechanism to use.)
- Encryption:** 3DES-168 (Specify the encryption mechanism to use.)
- IKE Proposal:** sonicwall (Select the IKE Proposal to use for this LAN-to-LAN connection.)
- Routing:** None (Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.)

Below the main configuration fields is the "Local Network" section:

- Network List:** Use IP Address/Wildcard-mask below (Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.)
- IP Address:** 192.168.30.0 (Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore.)

The left sidebar contains a navigation tree with categories: Configuration, Administration, and Monitoring. The "Configuration" category is expanded to show "Tunneling Protocols" and "IPSec". The "IPSec" category is further expanded to show "LAN-to-LAN".

Creating IKE IPSec VPN Tunnels between SonicWALL Devices and Cisco 3000 VPN Concentrators

Sample of IPSec LAN-to-LAN Setup (bottom half):

The screenshot shows the configuration page for an IPSec LAN-to-LAN connection in the Cisco VPN 3000 Concentrator Series Manager. The browser window title is "Cisco Systems, Inc. VPN 3000 Concentrator [tarantula] - Microsoft Internet Explorer". The address bar shows "http://192.168.30.1/access.html". The page header includes "VPN 3000 Concentrator Series Manager" and "Logged in: admin".

**Configuration**

- Interfaces
- System
- Servers
- Address Management
- Tunneling Protocols
  - PPTP
  - L2TP
  - IPSec
    - LAN-to-LAN
    - IKE Proposals
    - IPSec over TCP
- IP Routing
- Management Protocols
- Events
- General
- Client Update
- Load Balancing
- User Management
- Policy Management

**Administration**

**Monitoring**

**IPSec LAN-to-LAN Configuration:**

- Preshared Key:** 4k#Tama49
- Authentication:** ESP/MD5/HMAC-128
- Encryption:** 3DES-168
- IKE Proposal:** sonicwall
- Routing:** None

**Local Network:**

- Network List:** Use IP Address/Wildcard-mask below
- IP Address:** 192.168.30.0
- Wildcard Mask:** 0.0.0.255

**Remote Network:**

- Network List:** Use IP Address/Wildcard-mask below
- IP Address:** 192.168.76.0
- Wildcard Mask:** 0.0.0.7

Buttons: Apply, Cancel

Creating IKE IPSec VPN Tunnels between SonicWALL Devices and Cisco 3000 VPN Concentrators

Sample of Configured SA:

The screenshot shows the 'VPN 3000 Concentrator Series Manager' web interface. The left-hand navigation tree is expanded to 'IPSec' > 'LAN-to-LAN' > 'IPSec over TCP'. The main content area is titled 'Modify a configured Security Association.' and contains the following configuration fields:

- SA Name:** L2L: tosonicwall (Specify the name of this Security Association (SA).)
- Inheritance:** From Rule (Select the granularity of this SA.)
- IPSec Parameters:**
  - Authentication Algorithm:** ESP/MD5/HMAC-128 (Select the packet authentication algorithm to use.)
  - Encryption Algorithm:** 3DES-168 (Select the ESP encryption algorithm to use.)
  - Encapsulation Mode:** Tunnel (Select the Encapsulation Mode for this SA.)
  - Perfect Forward Secrecy:** Disabled (Select the use of Perfect Forward Secrecy.)
  - Lifetime Measurement:** Time (Select the lifetime measurement of the IPSec keys.)
  - Data Lifetime:** 10000 (Specify the data lifetime in kilobytes (K.B).)
  - Time Lifetime:** 86400 (Specify the time lifetime in seconds.)
- IKE Parameters:**
  - IKE Peer:** 65.70.200.57 (Specify the IKE Peer for a LAN-to-LAN IPSec connection.)
  - Negotiation Mode:** Main (Select the IKE Negotiation mode to use.)
  - Digital Certificate:** None (Use Preshared Keys) (Select the Digital Certificate to use.)
  - Certificate Transmission:**  Entire certificate chain,  Identity certificate only (Choose how to send the digital certificate to the IKE peer.)
  - IKE Proposal:** sonicwall (Select the IKE Proposal to use as IKE initiator.)

Buttons for 'Apply' and 'Cancel' are located at the bottom of the configuration area.