

# Tech Note

## Introduction

This technote can be used to help troubleshoot some of the most commonly-reported issues with site-to-site VPN setup on SonicWALL Security Appliances. If you are experiencing issues, please review this document before contacting SonicWALL technical support.

If you are configuring a site-to-site VPN tunnel between a SonicWALL security appliance and a third-party VPN device, please check the following documentation sites before continuing, as SonicWALL maintains a number of interoperability guides for other manufacturers' devices: <http://www.sonicwall.com/us/support/323.html>. The information contained in this technote may be useful when troubleshooting interoperability issues, but does not specifically cover interoperability as a topic.

For technical details on SonicWALL's IKE/IPsec functionality, please refer to the 'SonicWALL IKE/IPsec Implementation FAQ', which can be found here: [http://www.sonicwall.com/downloads/IKE\\_IPSec\\_Implementation\\_FAQ.pdf](http://www.sonicwall.com/downloads/IKE_IPSec_Implementation_FAQ.pdf).

## Recommended Versions

- SonicOS Standard 3.1.0.7 and newer
- SonicOS Enhanced 3.1.0.7 and newer
- Firmware 6.6.x and newer (*for older GEN3-series security appliances*)

Customers with current service/software support contracts can obtain updated versions of SonicWALL software images from the MySonicWALL customer portal at <https://www.mysonicwall.com>. Updated software images are also freely available to customers who have registered the SonicWALL security appliance on MySonicWALL for the first 90 days for TZ 170-series and PRO-series, and the first 30 days for TZ 150-series.

## Troubleshooting Checklist

**Before You Begin:** On the SonicWALL security appliance, enable all log categories, regardless of SonicWALL OS (6.x firmware, SonicOS Standard, SonicOS Enhanced); if SonicOS Enhanced, set for level 'debug'. This will greatly assist you during troubleshooting. Also, before you modify settings, make sure to export the preferences, TSRs, and firmware from the SonicWALLs and store them in a safe place. When done troubleshooting, return the log settings to less-verbose settings appropriate for your networking environment.

## Problem #1: All of the applications I'm running across the VPN tunnel keep dropping, or the VPN tunnel itself is dropping...I'm not sure which.

**Possible solution:** This issue is seen mostly with SonicOS Enhanced; it's not actually the VPN tunnel dropping, but rather the default TCP lifetime for the tunnel is set too low. On most SonicWALLs, its set for 5 minutes by default, which usually is not enough time for some applications and will disconnect a connection it sees as an open TCP connection (i.e. your applications) as inactive. Unlike SonicOS Enhanced, Firmware 6.x and SonicOS Standard do not run VPN traffic through NAT or the full stateful or deep packet inspection engines, and thus do not subject it to connection timeouts unless the 'Apply NAT and Firewall Rules' option is enabled. To remedy this issue, adjust the lifetimes on both sides of the VPN tunnel. For each SonicWALL OS type, here's how:

- **Firmware 6.6.x (only if 'Apply NAT and Firewall Rules' is enabled)** – Log into the SonicWALL's Management GUI. Go to the 'Access > Rules' page. For both of the 'Key Exchange (IKE)') rules, click on the 'Configure' icon to the right and adjust the 'Inactivity timeout in Minutes' field from the default of '5' to '60'. When done, click on the 'OK' button to save and activate the changes. NOTE: Do not adjust the 'Network Connection Inactivity Timeout (minutes)' entry field found on the 'Access > Services' page, as this applies to every connection through the SonicWALL, and may cause the connection cache to fill up and prevent subsequent connections.



## Tech Note

---

- SonicOS Standard (only if 'Apply NAT and Firewall Rules' is enabled) -- Log into the SonicWALL's Management GUI. Go to the 'Firewall > Access Rules' page. For both of the 'Key Exchange (IKE)" rules, click on the 'Configure' icon to the right and click on the 'Advanced' tab. From there, adjust the 'TCP Connection Inactivity Timeout (minutes)' field from the default of '5' to '60'. When done, click on the 'OK' button to save and activate the changes. NOTE: Do not adjust the 'Default Connection Timeout (minutes)' entry field found on the 'Firewall > Advanced' page, as this applies to every connection through the SonicWALL, and may cause the connection cache to fill up and prevent subsequent connections.
- SonicOS Enhanced -- Log into the SonicWALL's Management GUI. Go to the 'Firewall > Access Rules' page and choose the 'Matrix' view style. Click on the configure icon for the 'LAN > VPN' zone intersection. On the page that appears, you will see rules for the SonicWALL's subnets to the remote SonicWALL's subnets that were auto-created when you created the VPN policy. For these rules (there may be more than one), click on the 'Configure' icon at the right and click on the 'Advanced' tab. From there, adjust the 'TCP Connection Inactivity Timeout (minutes)' field from the default of '5' to '60'. When done, click on the 'OK' button to save and activate the changes.

Return to the 'Matrix' view style and click on the configure icon for the 'VPN > LAN' zone intersection. On the page that appears, you will see rules for the remote SonicWALL's subnets to the SonicWALL's LAN subnets that were auto-created when you created the VPN policy. For these rules (there may be more than one), click on the 'Configure' icon at the right and click on the 'Advanced' tab. From there, adjust the 'TCP Connection Inactivity Timeout (minutes)' field from the default of '5' to '60'. When done, click on the 'OK' button to save and activate the changes.

If your VPN tunnel terminates to zones other than the LAN, you will need to also adjust those rules in both directions.

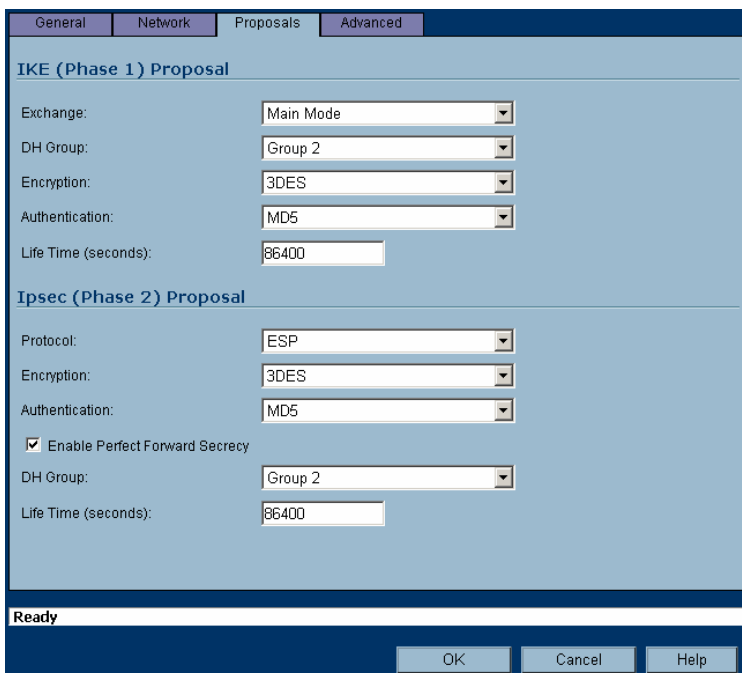
**NOTE:** Be careful adjusting the 'Default Connection Timeout (minutes)' entry field found on the 'Firewall > TCP Settings' page (or if it's SonicOS Enhanced 2.5, the 'Firewall > Advanced' page), as this applies to every connection through the SonicWALL, and may cause the connection cache to fill up and prevent subsequent connections. Please note that on both SonicOS Standard and SonicOS Enhanced, changing the 'Default Connection Timeout' has no effect on existing Access Rules – it only affects Access Rules created after the change (i.e. only the new rules inherit the new setting, old rules remain unchanged).

## Tech Note

### **Problem #2: I tried the solution above, but it looks like the VPN tunnel really is down – it was up for a while but now it no longer works.**

**Possible solution:** There may be default settings on the SonicWALL that are causing it to prematurely tear down a VPN policy before the lifetime expires. To amend this, please adjust the following:

VPN Policy Lifetime – The default lifetime for each individual VPN Policy is set to 28,800 seconds (8 hours). To make VPN policies last longer before they time out, log into the SonicWALL and click on the 'Configure' icon for the VPN Policy to the remote SonicWALL. On the page that appears, go to the 'Proposals' tab and adjust each 'Life Time (seconds)' field to a longer setting, such as '86400'. This change must be made on both sides; if they do not match, the devices will negotiate the lower of the two settings. For an example, see Figure 1:



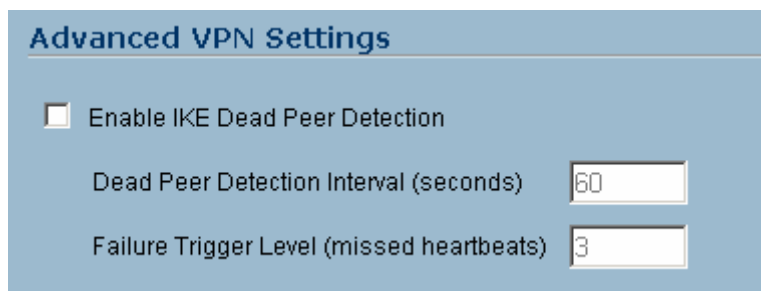
The screenshot shows the 'Advanced' tab of the 'Proposals' configuration page. It is divided into two sections: 'IKE (Phase 1) Proposal' and 'Ipsec (Phase 2) Proposal'. In the IKE section, the 'Life Time (seconds)' field is set to 86400. In the Ipsec section, the 'Life Time (seconds)' field is also set to 86400. Other settings include Exchange: Main Mode, DH Group: Group 2, Encryption: 3DES, and Authentication: MD5. The 'Enable Perfect Forward Secrecy' checkbox is checked. At the bottom, there are 'OK', 'Cancel', and 'Help' buttons.

Section	Field	Value	
IKE (Phase 1) Proposal	Exchange:	Main Mode	
	DH Group:	Group 2	
	Encryption:	3DES	
	Authentication:	MD5	
	Life Time (seconds):	86400	
Ipsec (Phase 2) Proposal	Protocol:	ESP	
	Encryption:	3DES	
	Authentication:	MD5	
	<input checked="" type="checkbox"/> Enable Perfect Forward Secrecy		
	DH Group:	Group 2	
	Life Time (seconds):	86400	

Figure 1 – Adjusting the VPN Policy lifetime to a longer value

## Tech Note

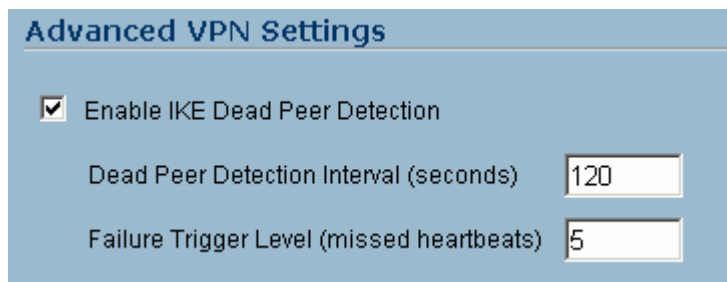
Dead Peer Detection – By default the SonicWALL is configured to perform ‘Dead Peer Detection’, which is a method to determine if the remote peer of a VPN policy is still active. By default the SonicWALL will send a small “are you there?” packet every sixty seconds. If the remote SonicWALL fails to respond to three of these packets (also the default setting), the SonicWALL will tear down the VPN tunnel. Sometimes these packets get lost, and sometimes the timers are set too short, but the result is the SonicWALL tears down a VPN tunnel that actually had no problems. You can try to fix this by doing two things – you can either shut off DPD on both sides, or you can adjust the DPD timers so that they are less aggressive. For example, to shut off DPD completely, go to the ‘VPN > Advanced’ page and uncheck the box next to ‘Enable IKE Dead Peer Detection’. Make sure to do this on at least one side of the tunnel (for performance reasons, you may wish to not enable DPD on a SonicWALL that’s terminating many VPN policies). For an example, see Figure 2 below.



The screenshot shows the 'Advanced VPN Settings' section. The 'Enable IKE Dead Peer Detection' checkbox is unchecked. Below it, the 'Dead Peer Detection Interval (seconds)' is set to 60, and the 'Failure Trigger Level (missed heartbeats)' is set to 3.

Figure 2 – Disabling Dead Peer Detection

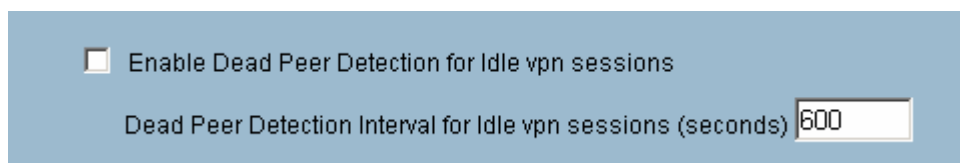
If you find DPD useful (and it is), but simply want to adjust the timers, experiment with the Interval and Trigger Level (again, on both sides) until the VPN tunnel stops dropping. For an example of a SonicWALL set to send an “are you there?” every two minutes and to tear the VPN tunnel down after five consecutive missed replies (10 minutes total), see Figure 3:



The screenshot shows the 'Advanced VPN Settings' section. The 'Enable IKE Dead Peer Detection' checkbox is checked. Below it, the 'Dead Peer Detection Interval (seconds)' is set to 120, and the 'Failure Trigger Level (missed heartbeats)' is set to 5.

Figure 3 – Adjusting the Dead Peer Detection timers

Another setting that may cause issues is the ‘Enable Dead Peer Detection for Idle vpn sessions’ function, which is found on the same page (see Figure 4 below). This feature is only in SonicOS Enhanced and is not in older firmware 6.x or SonicOS Standard. By default this option is disabled. This feature will tear down a VPN policy only if the peer stops responding to DPD requests. If there has been traffic activity on the VPN policy, the peer liveliness is implicit. This setting controls whether or not the DPD requests will be sent periodically on a policy that has seen no traffic activity. Unless your SonicWALL has a lot of remote sites and you’ve been advised to use this function, please do not enable it.



The screenshot shows the 'Advanced VPN Settings' section. The 'Enable Dead Peer Detection for Idle vpn sessions' checkbox is unchecked. Below it, the 'Dead Peer Detection Interval for Idle vpn sessions (seconds)' is set to 600.

Figure 4 – Disabling DPD for idle VPN sessions

## Tech Note

Keep Alive – In the VPN policy, this setting, if enabled, causes the SonicWALL to automatically negotiate a VPN tunnel and keep it permanently up (aka a ‘nailed up’ connection). By default this setting is disabled, which means that a VPN tunnel will only negotiate when the SonicWALL receives traffic destined for the network(s) behind the remote peer VPN gateway, and will keep the VPN tunnel active until the lifetime expires. To use this feature, click on the ‘Configure’ icon for the VPN policy and go to the ‘Advanced’ tab. Check the box next to ‘Enable Keep Alive’. If the device is running SonicOS Standard, it has a sub-option to ‘Try to bring up all possible tunnels’ – check this box as well. For an example, see Figure 5 below. When done, click on the ‘OK’ button to save and activate the changes. NOTE: it’s strongly recommended that this feature only be enabled on \*one\* side of the VPN tunnel – generally the smaller of the two sites of the VPN policy, and especially on sides that have dynamically-obtained WAN IP addresses. For example, a home SonicWALL TZ 170 with a PPPoE connection connecting to a central office PRO 4060 – Keep Alives would only be enabled on the home TZ 170.

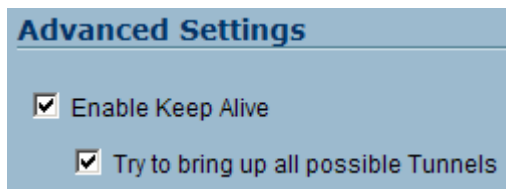


Figure 5 – Enabling Keep Alive to negotiate all subnets

Clean up Active Tunnels – By default, the SonicWALL has the ‘Clean up Active tunnels when Peer Gateway DNS name resolves to a different IP Address’ feature enabled. The SonicWALL uses this when a VPN policy has been created and enabled that uses a fully-qualified domain name (FQDN) for the peer IPsec Gateway. This feature is most useful when the remote peer has a dynamic WAN IP address mapped to a Dynamic DNS name, and that IP address changes frequently. The SonicWALL will resolve FQDNs to determine if the IP has changed when the DNS TTL expires, and also when renegotiating VPN policies. The feature causes the SonicWALL to periodically query the DDNS record – if the IP address changes, the VPN tunnel will immediately be torn down. If neither side of the VPN tunnel has a dynamic WAN IP address, or if neither side is using FQDNs for the IPSEC Gateway, this feature should be deactivated. To deactivate it, go to the ‘VPN > Advanced’ page and uncheck the box next to ‘Clean up Active tunnels when Peer Gateway DNS name resolves to a different IP Address’ on each SonicWALL. When done, click on the ‘OK’ button to save and activate the changes.

### **Problem #3: I configured the VPN Policy but it’s not connecting at all – nothing is happening, or there are some strange messages about “Phase 1” in the logs.**

**Possible solutions:** For a VPN tunnel to successfully negotiate, a number of settings must EXACTLY MATCH on both sides, otherwise the tunnel will fail to negotiate. Below are a number of settings to check on both sides.

The easy stuff – is VPN actually enabled on the SonicWALL? It should be by default but sometimes settings get shut off inadvertently. Go to the ‘VPN > Settings’ page and make sure the checkbox next to ‘Enable VPN’ is checked (see Figure 6 below). Also, make sure the ‘Enable’ checkbox to the right of your VPN Policy is also checked.

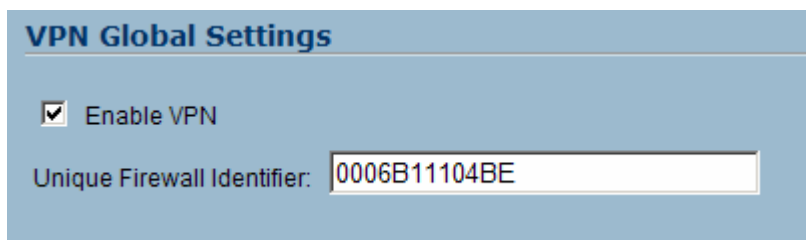


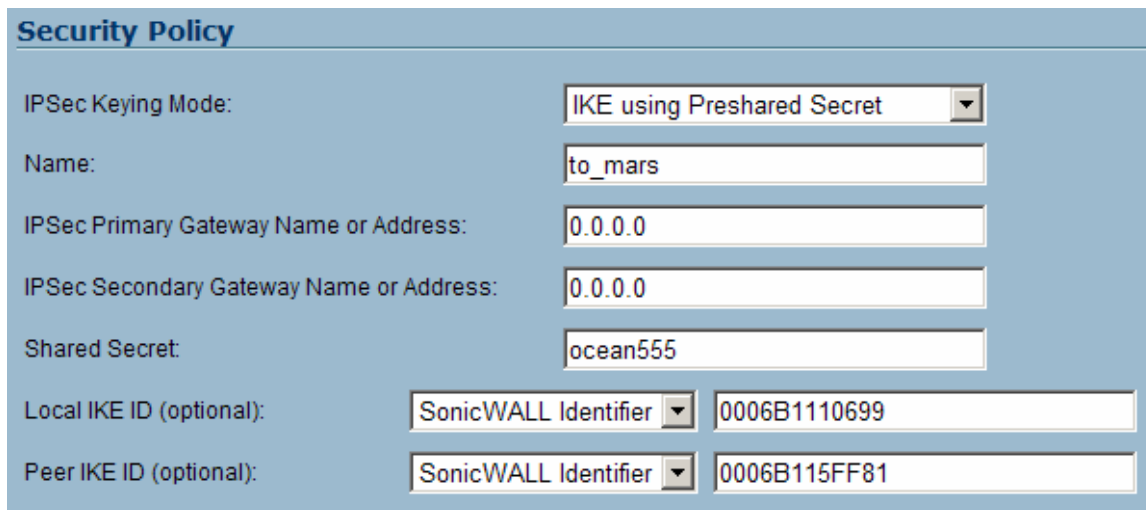
Figure 6 – The SonicWALL UFI

## Tech Note

Incorrect UFI Settings - If one side of the VPN tunnel is a SonicWALL whose WAN IP address is being obtained dynamically, then Aggressive Mode must be used. How to configure site-to-site SonicWALLs for VPN tunnels when one side is dynamic is outside of the scope of this troubleshooting document, but is covered here:

[http://www.sonicwall.com/downloads/configuring\\_vpns\\_between\\_sonicos\\_standard\\_and\\_sonicos\\_enhanced.pdf](http://www.sonicwall.com/downloads/configuring_vpns_between_sonicos_standard_and_sonicos_enhanced.pdf).

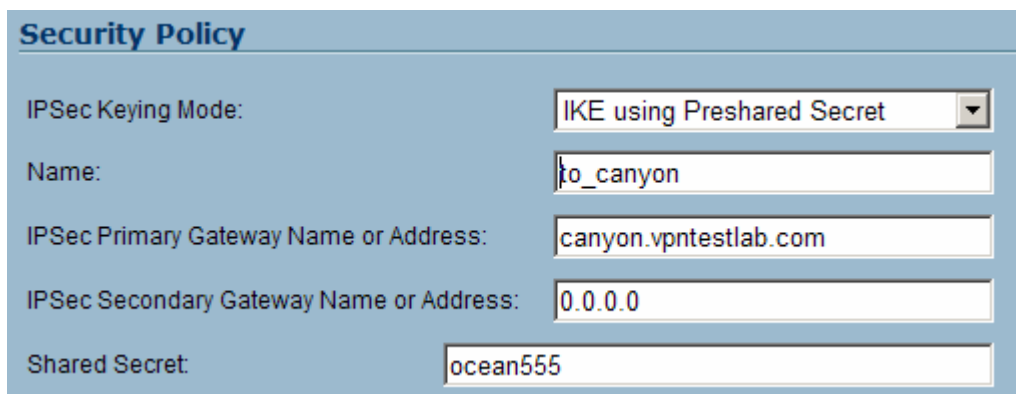
What is important to know is that the SonicWALL, when negotiating Aggressive Mode VPN tunnels, uses the 'Unique Firewall Identifier' (see Figure 6 above) as its identity. Both sides must be set to know the other side's UFI. In the older 6.x firmware and SonicOS Standard, this is done by naming the VPN Policy with the remote peer's UFI (and likewise). In SonicOS Enhanced it's controlled by setting the Local and Peer IKE ID's in the VPN policy's 'General' tab. For an example, see Figure 7:



The screenshot shows the 'Security Policy' configuration page. The 'IPSec Keying Mode' is set to 'IKE using Preshared Secret'. The 'Name' is 'to\_mars'. The 'IPSec Primary Gateway Name or Address' and 'IPSec Secondary Gateway Name or Address' are both set to '0.0.0.0'. The 'Shared Secret' is 'ocean555'. The 'Local IKE ID (optional)' is set to 'SonicWALL Identifier' with the value '0006B1110699'. The 'Peer IKE ID (optional)' is set to 'SonicWALL Identifier' with the value '0006B115FF81'.

Figure 7 – VPN Policy Aggressive Mode using UFIs

General Security Policy Settings – On the VPN policy's 'General' tab, make sure the 'IPSec Keying Mode' is set the same on both sides, and make sure you have the correct IP address or FQDN for the remote peer -- this one is a common mistake. Also make sure you have the same shared secret set on both sides (another common mistake -- if you see a log message on the SonicWALL that says 'Failed payload verification after decryption. Possible preshared key mismatch' or 'Received Notify: PAYLOAD\_MALFORMED, this is why). For an example, see Figure 8:

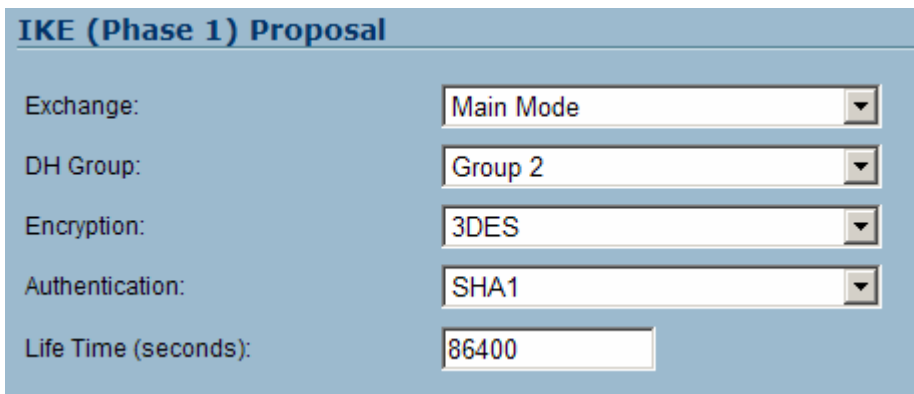


The screenshot shows the 'Security Policy' configuration page. The 'IPSec Keying Mode' is set to 'IKE using Preshared Secret'. The 'Name' is 'to\_canyon'. The 'IPSec Primary Gateway Name or Address' is 'canyon.vpntestlab.com'. The 'IPSec Secondary Gateway Name or Address' is '0.0.0.0'. The 'Shared Secret' is 'ocean555'.

Figure 8 – VPN Policy general settings

## Tech Note

**Phase 1 Settings** - If the SonicWALL's logs show messages that say "NO\_PROPOSAL\_CHOSEN", "IKE proposal does not match", or "IKE negotiation aborted due to timeout", the Phase 1 settings are probably incorrectly set on either side (or perhaps both). Most settings in the 'Proposals' tab of the VPN policy must EXACTLY MATCH on each side – if they do not the tunnel will fail not only Phase 1, but Phase 2 as well. The only exception is the 'Life Time' – if these do not match, the VPN policy will negotiate using the lower of the two settings. For an example of Phase 1 settings, see Figure 9:



Exchange:	Main Mode
DH Group:	Group 2
Encryption:	3DES
Authentication:	SHA1
Life Time (seconds):	86400

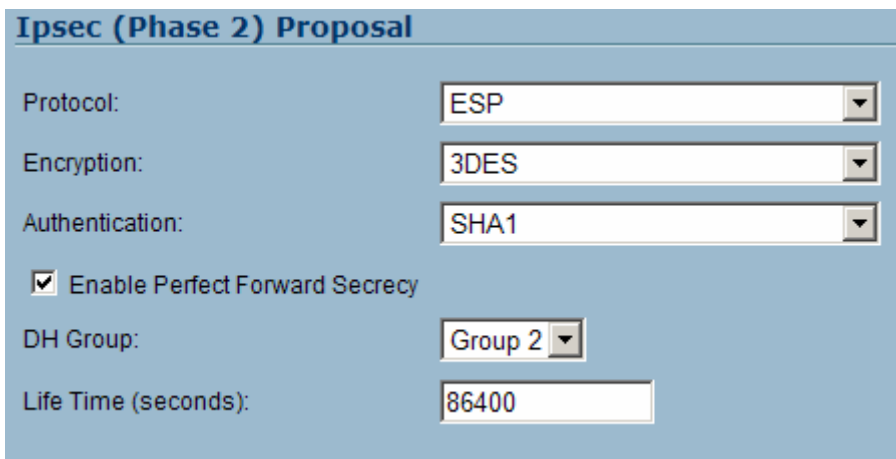
Figure 9 – VPN policy Phase 1 settings

**Firewall/Router in between** – If you've done all of the above and nothing seems to be happening, you may have something in between the two VPN devices that's blocking communication. If this is the case, make sure NAT Traversal is enabled on both SonicWALL devices, and that any firewall in between is set to pass UDP port 500 and UDP port 4500. If one of the sides is not a SonicWALL device, it will be necessary to open UDP port 500 and IP type 50, since NAT Traversal may not negotiate with the third-party device.

### **Problem #4: OK, I made sure the Phase 1 settings are set identically on both sides, and now the logs say its failing "Phase 2" – what now?**

**Possible Solutions:** For a VPN tunnel to successfully negotiate, most of the settings must EXACTLY MATCH on both sides, otherwise the tunnel will fail to negotiate. Below are a number of settings to check on both sides.

**Phase 2 Basic Settings Mismatch** – Make sure both sides have their 'Protocol', 'Encryption', and 'Authentication' settings set to match, or the tunnel will fail. These settings are found by clicking the 'Configure' icon next to the VPN policy and clicking on the 'Proposals' tab. For an example see Figure 10:



Protocol:	ESP
Encryption:	3DES
Authentication:	SHA1
<input checked="" type="checkbox"/> Enable Perfect Forward Secrecy	
DH Group:	Group 2
Life Time (seconds):	86400

Figure 10 – Phase 2 Settings

## Tech Note

Perfect Forward Secrecy (PFS) Mismatch – By default, this feature is disabled on all SonicWALL devices. PFS is an additional security mechanism in IPsec that adds another layer of security to the VPN tunnel. If you're going to use it, make sure to check the box next to 'Enable Perfect Forward Secrecy' on the VPN policy's 'Proposals' tab, make sure the 'DH Group' matches, and make sure the 'Life Time (seconds)' field entry matches on both sides. Please note that if the 'Life Time' settings do not match, the VPN policy will negotiate using the lower of the two settings. For an example, see Figure 10 on the previous page.

Incorrect destination network(s) - Another variation in this case is: Side A has more local networks and does not match one-to-one the destinations networks configured on the peer and keep alive is enabled on side A. This will cause some Phase 2 to come up and the others will constantly cause NO PROPOSAL CHOSEN.

Missing 'Default LAN Gateway' Option – If the one side of the VPN tunnel is using the 'Use this VPN Tunnel as default route for all Internet traffic' option (also referred to as 'tunnel all'), it requires that a LAN default gateway be specified on the other side's VPN setup – but only if the main site is running SonicOS Standard or Firmware 6.x. This LAN default gateway cannot be the LAN IP address of the SonicWALL, and must be a separate internal router residing on the other side's LAN segment. To configure this feature, log into the main site's SonicWALL, go to the 'VPN > Settings' page, click the 'Configure' icon next to the VPN policy to the remote site that will be doing tunnel-all to the main site, and go to the 'Advanced' tab. In the field next to 'Default LAN Gateway', enter the IP address of the third-party router on the main SonicWALL's LAN segment. When done, click on the 'OK' button to save and activate the changes. This is not necessary when using SonicOS Enhanced.

Last packet of QM mode lost in transit – This was an infrequently-seen bug in older versions of SonicWALL firmware. If you are experiencing this problem, please upgrade to firmware 6.6.x, SonicOS Standard 3.1.0.6, or SonicOS Enhanced 3.1.0.6 to resolve this issue.

### **Problem #5: I've double- and triple-checked the General, Phase 1, and Phase 2 settings on both sides and it STILL won't negotiate!**

**Possible Solution:** If you've done all of the above and nothing seems to be happening, you may have something in between the two VPN devices that's blocking communication. Unfortunately this is hard to determine, since portions of the network path between the two VPN devices may lie underneath the control of external parties, who may or may not be helpful.

If this is the case, make sure NAT Traversal is enabled on both SonicWALL devices, and that any firewall/router/NAT device in between is set to pass UDP port 500 and UDP port 4500. If one of the sides is not a SonicWALL device, it will also be necessary to open UDP port 500 and IP type 50, since NAT Traversal may not negotiate with the third-party device.

### **Problem #6: The VPN Tunnel negotiated fine, and both sides show the tunnel as up, but I can't reach anything on either side of the tunnel from the other side, respectively – why?**

**Possible Solutions:** This problem manifests itself in several ways, so check all steps below to see if one or more of these is causing the connection issues.

Fragmentation Issues – See steps in Problem #7 on the next page.

DHCP MTU Issues – If the SonicWALL's WAN interface is receiving its IP address dynamically via DHCP, it may be necessary to lower the WAN interface's MTU. DHCP is common among cable ISPs, and many of them require unconventionally low MTU settings.

- If the SonicWALL runs the older 6.6.x firmware, log into the SonicWALL's Management GUI, go to the 'Advanced > Ethernet' page, adjust the 'WAN MTU' from '1500' to '1404', and click the 'Update' button to save and activate the change.
- If the SonicWALL runs SonicOS Standard, log into the SonicWALL's Management GUI, go to the 'Network > Settings' page, click on the 'Configure' icon next to the 'WAN' interface. On the page that appears, click on the





## Tech Note

'Ethernet' tab, adjust the 'WAN MTU' from '1500' to '1404', then click the 'OK' button to save and activate the change.

- If the SonicWALL runs SonicOS Enhanced, log into the SonicWALL's Management GUI, go to the 'Network > Interfaces' page, click on the 'Configure' icon next to the 'WAN' interface. On the page that appears, click on the 'Advanced' tab, adjust the 'Interface MTU' from '1500' to '1404', then click the 'OK' button to save and activate the change.

User-Level Authentication – ULA may have inadvertently been activated. If the SonicWALL is running older firmware 6.x or SonicOS Standard, check the 'Advanced' settings for the VPN policy to ensure that this feature is off (there are two checkboxes for 'Require Authentication of Local Users' and 'Require Authentication of Remote Users').

AV Enforcement – In SonicOS Enhanced, it's possible to enforce that the SonicWALL desktop anti-virus client be installed before allowing access to the network. This setting may have inadvertently been enabled. Go to the 'Network > Zones' page and click the 'Configure' icon next to the 'VPN' zone. If the check box next to 'Enforce Network Anti-Virus Service' is checked, uncheck it, and click on the 'OK' button to save and activate the change.

TCP Settings – Some applications do not work with the default TCP enforcement settings on the SonicWALL. It may be necessary to deactivate one or more of these settings on both sides of the VPN tunnel.

- If the SonicWALL runs the older 6.6.x firmware, log into the SonicWALL's Management GUI, and when the page appears, modify the URL from '/management.html' to '/diag.html.' This will open a hidden Diagnostics Settings Menu. When this menu appears click on the 'Internal Settings' button to the right. On this menu, uncheck the box next to 'Enable TCP Handshake Enforcement'. When done, click on the 'Submit' button in the upper-right-hand corner to apply and save the change.
- If the SonicWALL runs SonicOS Standard, log into the SonicWALL's Management GUI, and when the page appears, modify the URL from '/main.html' to '/diag.html.' This will open a hidden Diagnostics Settings Menu. When this menu appears click on the 'Internal Settings' button to the left. On this menu, uncheck the box next to 'Enable TCP Handshake Enforcement'. When done, click on the 'Apply' button in the upper-right-hand corner to apply and save the change, then click on the 'Close' button in the lower-left-hand corner to return to the SonicWALL's main management menu. **NOTE:** in newer versions of SonicOS Standard, the checkbox for 'Enable TCP Handshake Enforcement' is instead located on the 'Firewall > Advanced' page.
- If the SonicWALL runs SonicOS Enhanced, log into the SonicWALL's Management GUI, go to the 'Firewall > TCP Settings' menu, and uncheck the boxes next to 'Enable TCP Stateful Inspection' and 'Enable TCP Checksum Validation'. When done, click on the 'Apply' button in the upper-right-hand corner to save and activate the changes. There are three additional IP/TCP/UDP enforcement options on the 'Firewall > Advanced' page that you may also wish to deactivate.

Hardware Accelerated Cryptographic Miscalculations-- If you are using a SonicWALL TZ 170, and the VPN tunnel negotiates successfully but still does not pass traffic across the VPN tunnel, and the log is filled with 'IPSec Authentication Failed' messages, the onboard hardware crypto acceleration chip may have not be processing traffic correctly.

To remedy this, log into the SonicWALL's management GUI, and when the page appears, modify the URL from '/main.html' to '/diag.html.' This will open a hidden Diagnostics Settings Menu. When this menu appears click on the 'Internal Settings' button to the left. On this menu, uncheck the boxes next to the following (the last one is only in SonicOS Enhanced):

- Enable inbound VPN hardware acceleration (if available)
- Enable outbound VPN hardware acceleration (if available)
- Enable Asymmetric algorithm (DH and RSA) hardware acceleration (if available)

When done, click on the 'Apply' button in the upper-right-hand corner to apply and save the change, then click on the 'Close' button in the lower-left-hand corner to return to the SonicWALL's main management menu, and restart the SonicWALL for the changes to take effect. With these settings disabled, the SonicWALL will perform all crypto in software, which will reduce VPN throughput but will still be functional. **NOTE:** If disabling hardware crypto fixes the problem, please contact SonicWALL tech support to arrange for further diagnostics.



### **Problem #7: The VPN tunnel now works fine but it's, really, \*REALLY\* slow --- any way to make it go faster?**

**Possible Solution:** This is a tricky topic. Ultimately, your VPN tunnel is going to be limited by the slowest point between the two links. This is often referred to as the 'chokepoint'. For example, if you have a VPN tunnel between a central office that has a 1.5Mbps T1 connection to the Internet and a remote office that has a 256Kbps ADSL connection to the Internet, the VPN tunnel is going to be constrained by the ADSL connection's speed – and also by any traffic flowing in/out of that connection at any time (meaning, if there's someone at that remote office downloading stuff off the Internet all day/night, then the VPN tunnel is going to suffer and be even slower). Also, distance may play a role in perceived throughput – the farther apart the two links, the slower it may seem, due to latency, potential for packet loss/retransmission, or transient traffic in between the two points.

However, there are some settings on the SonicWALL that may improve throughput. Below are some settings to experiment with – please note these will need to be enabled on \*both\* sides of the VPN tunnel.

**Firmware 6.6.x** – Log into the SonicWALL's Management GUI. Go to the 'VPN > Summary' page and check the box next to 'Enable Fragmented Packet Handling'. When done, click on the 'Update' button in the lower-right-hand corner to save and activate the change. Reboot the SonicWALL for the change to take effect.

**SonicOS Standard** – Log into the SonicWALL's Management GUI. Go to the 'VPN > Advanced' page and check the boxes next to 'Enable Fragmented Packet Handling' and 'Ignore DF (Don't Fragment) Bit'. When done, click on the 'Apply' button in the upper-right-hand corner to save and activate the change. Reboot the SonicWALL for the changes to take effect.

**SonicOS Enhanced** – Log into the SonicWALL's Management GUI. Go to the 'VPN > Advanced' page and check the boxes next to 'Enable Fragmented Packet Handling' and 'Ignore DF (Don't Fragment) Bit'. When done, click on the 'Apply' button in the upper-right-hand corner to save and activate the change. Reboot the SonicWALL for the changes to take effect.

Outside of that, it may be necessary to use SonicWALL's bandwidth management to prioritize VPN traffic. This topic is too extensive to go into detail here but is covered in the 3.1 Administrators guide, which can be found here:

<http://www.sonicwall.com/us/support/289.html>. Bidirectional bandwidth management for VPN policies is available only in SonicOS Enhanced.

**NOTE:** If you're using GEN3-series SonicWALL security appliances (TELE3, SOHO3, PRO230/330, GX, SOHO TZW), you may wish to lower the encryption and hashing methods on each side of the VPN tunnel. Most people err on the side of security and crank the settings up to most secure possible, but with older hardware this may dramatically slow down the throughput across the VPN tunnel. If you have tried the steps above and are still experiencing slow transfer speeds, try lowering the settings to levels that increase the VPN tunnel throughput but still provide an acceptable level of security appropriate to your networking environment

### **Problem #8: I have a hub-and-spoke network set up but the spokes can't reach the other spoke networks, only the networks behind the hub – why?**

**Possible Solution:** Hub and Spoke configurations can be fairly complex, both from the perspective of the hub and spoke sites, and their implementation differs from 6.x and SonicOS Standard to SonicOS Enhanced.

A technote on how to set up hub-and-spoke networks on SonicWALLs can be found here:

<http://www.sonicwall.com/us/support/323.html>.

### **Problem #9: The VPN tunnel is up but I can't see any computers or servers in the Network Neighborhood on the other side – why?**

**Possible Solution:** Some Microsoft networking environments rely heavily on NetBIOS broadcasts to advertise and locate network resources (servers, print devices, etc). On a local LAN segment, this works fine, as broadcasts are propagated to every node on the local segment. When the network segments are separated by a router, or a VPN tunnel, this mechanism fails, since routers and VPN devices generally are not configured to forward broadcasts to remote segments. And, since people tend to access Microsoft network resources by a friendly name instead of IP address, they're accustomed to finding these resources by clicking on the 'Network Neighborhood' or 'My Network Places' desktop icons, or by a mapped drive to the resources.

By default, SonicWALL devices are configured to not pass Microsoft NetBIOS broadcasts across VPN tunnels. Below, we will detail how to configure the SonicWALL to pass these broadcasts across the VPN tunnel bidirectionally, for each firmware type. Please note this will increase traffic across the VPN tunnel(s) in most environments. In larger environments it may lead to a substantial increase in traffic, and because of this is not recommended. Instead, it is recommended that the Microsoft networking environment be correctly configured using Active Directory and/or WINS services, which are components of Microsoft's Windows 2003 Server.

**NOTE:** Correct use of AD and/or WINS will minimize issues when attempting to access Microsoft network resources across VPN tunnels. Please refer to <http://support.microsoft.com/default.aspx?scid=kb:en-us:160177> for a more detailed discussion of this topic.

How to forward NetBIOS broadcasts across VPN site-to-site tunnels:

- **Firmware 6.6.x** – Log into the SonicWALL's Management GUI. Go to the 'VPN > Summary' page and uncheck the box next to 'Disable all VPN Windows Networking (NetBIOS) broadcast'. When done, click on the 'Update' button in the lower-right-hand corner of the page to save and activate the change. Now, go to the 'VPN > Configure' page. Use the pull-down menu next to 'Security Association' to select each VPN policy on the SonicWALL. For each VPN policy, click on the 'Advanced Settings' button at the bottom and check the box next to 'Enable Windows Networking (NetBIOS) broadcast'. When done, click on the 'OK' button to save and activate the change, and when you are returned to the 'VPN > Configure' page, click on the 'Update' button in the lower-right-hand corner of the page to save and activate the changes.
- **SonicOS Standard** - Log into the SonicWALL's Management GUI. Go to the 'VPN > Advanced' page and uncheck the box next to 'Disable all VPN Windows Networking (NetBIOS) broadcast'. When done, click on the 'Apply' button in the upper-right-hand corner of the page to save and activate the change. Now, go to the 'VPN > Configure' page. Click on the 'Configure' icon next to each active VPN policy on the SonicWALL. Click on the 'Advanced' tab for each policy and check the box next to 'Enable Windows Networking (NetBIOS) broadcast'. When done, click on the 'OK' button to save and activate the changes.
- **SonicOS Enhanced** – Log into the SonicWALL's Management GUI. Go to the 'VPN > Configure' page. Click on the 'Configure' icon next to each active VPN policy on the SonicWALL. Click on the 'Advanced' tab for each policy and check the box next to 'Enable Windows Networking (NetBIOS) broadcast'. When done, click on the 'OK' button to save and activate the changes. Now, go to the 'Network > IP Helper' page – you will see that the SonicWALL automatically created NetBIOS policies when you checked the boxes in the previous step. On this page, check the boxes next to 'Enable IP Helper' and 'Enable NetBIOS Support'. When done, click on the 'Apply' button in the upper-right-hand corner of the page to save and activate the change. Please note that SonicOS Enhanced doesn't support NetBIOS broadcasts over VPNs unless the network address objects on both sides are subnets, not IP ranges, single hosts, or groups containing them.
- NetBIOS support in SonicOS Enhanced is much more extensive than other SonicWALL OS's -- for an in-depth overview of the IP Helper feature please refer to the following document: [http://www.sonicwall.com/downloads/ip\\_helper.pdf](http://www.sonicwall.com/downloads/ip_helper.pdf).

## Problem #10: The VPN tunnel is up but some applications don't seem to work across the tunnel – why?

**Possible Solution:** Try the Fragmentation options detailed in Problem #7, and if the SonicWALL's WAN interface is receiving its IP address dynamically via DHCP, try the MTU options detailed in Problem #6.

## Problem #11: I am seeing a bunch of alert messages in the log about “VPN TCP SYN” – should I be worried or call tech support?

**Possible Solution:** These messages indicate that the 'VPN TCP Stats' category has been activated in the Log settings. Unfortunately, activating this category generates a lot of log messages unnecessarily tagged as alerts -- meaning, they show up in bright yellow in the logs and tend to alarm people (see Figure 11 below). All the messages mean is that the SonicWALL logged traffic across the VPN tunnel. This will be resolved in future releases of the older 6.6.x firmware and in SonicOS Standard. These messages do not appear in any version of SonicOS Enhanced.

7	07/15/2005 09:17:17.464	RECEIVED<<< ISAKMP OAK INFO (InitCookie 0x6c1b2e7987248c63, MsgID: 0x35354B5) *(HASH, NOTIFY:DPD_REQUEST)	67.115.118.71, 500	67.115.118.84, 500
8	07/15/2005 09:17:16.448	VPN TCP FIN	192.168.74.47, 4360, DAKOTA	192.168.168.168, 20480
9	07/15/2005 09:17:16.432	VPN TCP PSH	192.168.74.47, 4360, DAKOTA	192.168.168.168, 20480
10	07/15/2005 09:17:16.416	VPN TCP SYN	192.168.168.168, 20480	192.168.74.47, 4360, DAKOTA
11	07/15/2005 09:17:11.656	SENDING>>>> ISAKMP OAK INFO (InitCookie 0xa0a303906e4e2850, MsgID: 0x62ADDA61) *(HASH, NOTIFY:DPD_ACK)	67.115.118.84, 500	207.88.91.90, 500, 207.88.91.90.ptr.us.xo.net

Figure 11 – Unexplained VPN log messages

To stop these messages from appearing, go to 'Log > Categories' and uncheck the box next to 'VPN TCP Stats' in the 'Log Categories' section.

## Problem #12: My Site-to-Site VPN is working, but one or more of our servers or computers isn't reachable through the tunnel, or can't send traffic through the tunnel

### Possible Solutions:

1. In some networks, there are multiple paths to the internet from the LAN, and sometimes this problem is caused by a host whose default gateway isn't configured in such a way that it can participate in the VPN traffic. The problem computer may not have a default gateway set at all (common on platforms which don't offer GUI methods for setting gateways like Windows, and when the server historically has only been reached by local hosts on the same network). The answer is simply to configure a default gateway on the computer (or a route of last resort in a LAN router) equal to the SonicWALL LAN IP address. Some server platforms are set up by contractors or integrators and are not touched by the organization's IT staff until this type of problem arises. In fact, there may not be anybody onsite who is capable of determining the current IP configuration of that server.

For example, a LAN has two gateway devices:

- A Netgear router and

- A parallel SonicWALL VPN gateway,

each doing NAT and using internal IP addresses of 10.7.6.1 and 10.7.6.254, respectively.

The VPN peer network LAN is using an IP address scheme of 10.100.4.x / 24.

## Tech Note

The VPN tunnel is up, and a Windows workstation w/ IP address of 10.7.6.25 is accessible from computers on the VPN peer network. But two hosts are not reachable through the tunnel (a workstation w/ IP address of 10.7.6.155 and a Citrix server w/ IP address of 10.7.6.7), but both can be pinged from the SonicWALL on its LAN. Please note that a default gateway on the computer is not needed for it to be pingable by its LAN neighbors.

Using ipconfig output, the computer is found to be using a default gateway of the netgear router 10.7.6.1, and the Citrix server doesn't even have a gateway set.

2) AV enforcement may be enabled on the VPN zone in SonicOS Enhanced – check the head end's logs for dropped connections. If this is the case, the server's IP address will need to be added to the exclusion range.

3) Rarely, a computer will use multiple IP addresses, and sometimes it will have an IP address in both of the subnets used across the VPN tunnel. When that is true, any attempts to reach hosts on the other side will result only in a local ARP request by that computer on its own network for that host, since it has an IP in that target subnet.

### **Problem #13: My route-all VPN is working for access to the main LAN network, but the Internet isn't reachable through the tunnel, even though the IKE phase 2 negotiations on both sides clearly show that the spoke network is negotiated for all destinations (0.0.0.0 /0)**

For example, a SonicWALL VPN gateway, w/ a LAN IP address of 10.7.6.1 and WAN IP address of 67.115.118.253. The VPN peer network LAN is using an IP address scheme of 10.100.4.x / 24.

The computer w/ IP address of 10.100.4.200 on the spoke network is able to contact all devices on the other side of the VPN, but cannot reach the internet through its route all VPN policy to the head end VPN Gateway. Pings to reachable hosts like 4.2.2.2 fail, as do pings to the GW router above the head end SonicWALL.

**Possible Solution:** Have somebody on the head-end network log into the head-end SonicWALL, and do a packet trace (System - Diagnostics screen) on the destination IP address being pinged (e.g., 4.2.2.2). Have the spoke computer user do the ping, and then refresh the packet trace. This allows the head end SonicWALL to inspect the nature of the packets being sent out in the clear, if they are being sent. You may see something like this:

1. ICMP packet rec'd on LAN: source: 10.100.4.200 dest'n: 4.2.2.2
2. ICMP packet sent on WAN: source: 10.100.4.200 dest'n: 4.2.2.2

The head-end SonicWALL must have a NAT Policy which translates internet-bound traffic from the spoke network into a public IP address. Predictably, a NAT Policy will make the source of the 2nd packet in the trace a public IP address, so that it can be routed through their internet connection and back:

1. ICMP packet rec'd on LAN: source: 10.100.4.200 dest'n: 4.2.2.2
2. ICMP packet sent on WAN: source: 65.115.118.253 dest'n: 4.2.2.2
3. ICMP packet rec'd on WAN: source: 4.2.2.2 dest'n: 65.115.118.253



## Tech Note

### Common VPN Log Messages – And what they actually mean

Below are some of the most commonly-seen log messages relating to VPN negotiation problems, and explanations for each message that can be used to troubleshoot and resolve the issue.

LOG MESSAGE	DESCRIPTION
VPN TCP SYN	Device has encountered a SYN flag in a TCP stream across the VPN tunnel – this is not an error condition and is normal
VPN TCP FIN	Device has encountered a FIN flag in a TCP stream across the VPN tunnel – this is not an error condition and is normal
VPN TCP PSH	Device has encountered a PSH flag in a TCP stream across the VPN tunnel – this is not an error condition and is normal
XAUTH Failed with VPN Client; Authentication failure	Incoming VPN client user authentication, or site-to-site authentication has failed – user has either entered the incorrect username, or incorrect password
XAUTH Failed with VPN Client; Cannot contact RADIUS Server	Device cannot successfully contact external RADIUS server(s) for user/password authentication, for incoming VPN clients or site-to-site authentication
VPN Client Policy Provisioning	Device is downloading a connection policy to an incoming client VPN connection
Global VPN Client License Exceeded; Connection Denied	Device has either reached its global limit of allowable active client VPN connections, or its license limit – if the latter, device needs license upgrade installed
Blocked Quick Mode for Client using Default KeyId	Device is not allowing incoming client VPN (GVC) phase 2 negotiation using simple key; solution is to delete and re-add connection in GVC
Global VPN Client connection is not allowed. Appliance is not registered	Device must be fully registered at <a href="https://www.mysonicwall.com">https://www.mysonicwall.com</a> customer portal before it will allow incoming client VPN (GVC) connections
Global VPN Client version cannot enforce personal firewall. Minimum version required is 2.1	Device is enforcing Global Security Client option on group VPN policies and client is running standalone GVC and not GSC. Solution is not to run standalone GVC and install GSC (GVC 2.2 is a component of GSC).
IKE Responder: IP address already exists in the DHCP Relay table. Client traffic not allowed	Device has detected that GVC is proposing a virtual IP address that exists in DHCP Relay table. Solution is to change the virtual IP address on the GVC (only if statically assigned) so that it no longer conflicts with the existing entry in the DHCP Relay table.

## Tech Note

IKE Responder: %s policy does not allow static IP for virtual adapter	Incoming client VPN (GVC) connection is proposing a static virtual IP address, but the VPN policy has not been set to allow this. Solution is to modify VPN policy's 'Client' settings to allow 'DHCP Lease or Manual Configuration' for the Virtual Adapter.
IKE Responder: IPSec proposal does not match (phase 2)	Phase 2 settings proposed by IKE Initiator do not match those of the remote site (IKE Responder) – this can include mismatched destination networks, mismatched protocol settings, mismatched encryption settings, mismatched authentication settings, or mismatched PFS settings (one side enabled, one side not). Solution is to make sure all of the above match exactly on both peers of the VPN policy.
IKE Responder: Mode %d – not tunnel mode	Peer is attempting to negotiate using transport mode - SonicWALLs only support tunnel mode for VPNs. Solution is to configure peer to use tunnel mode.
IKE Responder: No matching phase 1 ID found for proposed remote network	IKE Phase 1 Identities are mismatched. See 'Troubleshooting Guide for IKE VPN Initialization for SonicOS' for steps on how to resolve this.
IKE Responder: Proposed remote network 0.0.0.0 but not DHCP relay nor default route	Peer is proposing tunnel-all, but other side is not configured for tunnel-all. Check Phase 2 VPN configuration on both peers.
IKE Responder: No match for proposed remote network address	Peer is proposing a Phase 2 destination network that is not configured in VPN policy. Check Phase 2 VPN configuration on both peers.
IKE Responder: Default LAN gateway is set but peer is not proposing to use this SA as a default route	Peer is *not* proposing tunnel-all, but other side is *is* configured for tunnel-all. Check Phase 2 VPN configuration on both peers.
IKE Responder: ESP Perfect Forward Secrecy mismatch	Peer is proposing PFS but other side's PFS settings are incorrectly configured. Check Phase 2 PFS settings on both peers.
IKE Responder: Algorithms and/or keys do not match	Peer is proposing encryption settings that do not match other side. Check Phase 2 Encryption settings on both peers.
IKE Responder: IKE proposal does not match (Phase 1)	Phase 1 settings proposed by IKE Initiator do not match those of the remote site (IKE Responder) – this can include mismatched IKE Identities, mismatched encryption settings, mismatched authentication settings, or mismatched DH Group. Solution is to make sure all of the above match exactly on both peers of the VPN policy.
IKE Initiator: Received notify. NO_PROPOSAL_CHOSEN	Responder is reporting that Phase 1 or Phase 2 settings are mismatched. Check Phase 1 and Phase 2 settings on both peers.
Received notify: ISAKMP_AUTH_FAILED	Responder is reporting that preshared key is mismatched. Check settings on both peers.

## Tech Note

Received notify: PAYLOAD_MALFORMED	Responder is reporting that it cannot decrypt the payload (an encrypted IKE packet); one side may have rebooted and no longer has correct IKE cookies. Solution is to reset VPN policy on both peers.
Received notify: INVALID_COOKIES	One side has rebooted and no longer has correct IKE cookies. Solution is to reset VPN policy on both peers.
Received notify: RESPONDER_LIFETIME	Responder is configured for a lower SA lifetime than the other peer. This is not an error condition and can be ignored.
Received notify: INVALID_SPI	One side has rebooted and no longer has correct IPsec SA. If DPD is enabled, SA will renegotiate. If DPD is not enabled, solution is to reset VPN policy.
IKE Responder: Proposed local network is 0.0.0.0 but SA has no LAN Default Gateway	Peer is proposing tunnel-all but other side is not configured with required LAN Default Gateway.
IKE Responder: Default LAN gateway is not set but peer is proposing to use this SA as a default route	Peer is proposing tunnel-all but other side is not configured with required LAN Default Gateway.
Received unencrypted packet while crypto active	One side has rebooted and no longer has correct IKE SA. If DPD is enabled, SA will renegotiate. If DPD is not enabled, solution is to reset VPN policy.
IKE ID mismatch %s	IKE Phase 1 Identities are mismatched. See 'Troubleshooting Guide for IKE VPN Initialization for SonicOS' for steps on how to resolve this.
Received notify: INVALID_PAYLOAD	One side has rebooted and no longer has correct IKE SA. If DPD is enabled, SA will renegotiate. If DPD is not enabled, solution is to reset VPN policy.
Illegal IPsec SPI	One side has rebooted and no longer has correct IKE SA. If DPD is enabled, SA will renegotiate. If DPD is not enabled, solution is to reset VPN policy.
Unknown IPsec SPI	One side has rebooted and no longer has correct IKE SA. If DPD is enabled, SA will renegotiate. If DPD is not enabled, solution is to reset VPN policy.
IPsec Authentication Failed	ESP Authentication has failed. Please refer to the 'Hardware Accelerated Cryptographic Miscalculations' section of this document if this message is seen repeatedly in the logs.
IPsec Decryption Failed	ESP Authentication has failed. Please refer to the 'Hardware Accelerated Cryptographic Miscalculations' section of this document if this message is seen repeatedly in the logs.



## Tech Note

Incompatible IPSec Security Association	One side has rebooted and no longer has correct IKE SA. If DPD is enabled, SA will renegotiate. If DPD is not enabled, solution is to reset VPN policy.
IPSec packet from or to an illegal host	Source and destination addresses do not match negotiated Phase 2 VPN policy settings.
IPSEC Replay Detected	Peer has sent an IPsec packet with a repeated sequence number and has dropped the repeated packet.
Received notify: INVALID_ID_INFO	Peer has responded that Phase 1 or Phase 2 settings are incorrect. Check Phase 1 and Phase 2 VPN policy settings on both peers.

### Contacting Tech Support

If the above sections do not adequately describe the issue you are experiencing, or if you have tried all steps above and are still experiencing problems, SonicWALL offers a wide range of support options, including online support documentation, real-time web-based support, online user discussion forums, and phone-based support. These options are available to you via the site listed below.

<http://www.sonicwall.com/support/contact.html>

Support is available for 30 days upon registration for SonicWALL TZ 150 and SonicWALL TZ 150W security appliances, and for 90 days upon registration for all other SonicWALL security appliances. Support is also available for customers with current and valid service & support contracts.

**Created: 07/12/2005**

**Updated: 09/10/2007**

**Version 1.2**

**Maintainer: Dave Parry**

