SONICWALL INTERNAL FAQ:

SonicWALL IKE/IPSec Implementation FAQ

Which VPN-related RFC's and drafts are supported in SonicWALL firmware?
In firmware 6.6, SonicOS 2.1 Standard, and SonicOS 2.1 Enhanced, the following are supported:
RFCs:

- The ESP DES-CBC Transform (RFC 1829)
- IP Encapsulating Security Payload (ESP) (RFC 1827) obsoleted by RFC 2406
- IP Authentication using Keyed MD5 (RFC 1828)
- IP Authentication Header (RFC 1826) obsoleted by RFC 2402
- Security Architecture for the Internet Protocol (RFC 1825) obsoleted by RFC 2401
- HMAC: Keyed-Hashing for Message Authentication (RFC 2104)
- HMAC-MD5 IP Authentication with Replay Prevention (RFC 2085)
- Security Architecture for the Internet Protocol (RFC 2401)
- The NULL Encryption Algorithm and Its Use With IPsec (RFC 2410)
- IP Security Document Roadmap (RFC 2411)
- IP Authentication Header (RFC 2402)
- The OAKLEY Key Determination Protocol (RFC 2412)
- The ESP CBC-Mode Cipher Algorithms (RFC 2451)
- The Use of HMAC-MD5-96 within ESP and AH (RFC 2403)
- The Use of HMAC-SHA-1-96 within ESP and AH (RFC 2404)
- The ESP DES-CBC Cipher Algorithm With Explicit IV (RFC 2405)
- IP Encapsulating Security Payload (ESP) (RFC 2406)
- The Internet IP Security Domain of Interpretation for ISAKMP (RFC 2407)
- Internet Security Association and Key Management Protocol (ISAKMP) (RFC 2408)
- The Internet Key Exchange (IKE) (RFC 2409)
- More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE) (RFC 3526)
- The AES-CBC Cipher Algorithm and Its Use with IPsec (RFC 3602) (30254 bytes)

Internet Drafts:

- 'Negotiation of Nat-Traversal in the IKE'

What VPN enhancements are in SonicOS Standard/Enhanced?
Note the following:

- Ability to set individual Phase 2 lifetime
- Ability to set IKE Identity type and value (Enhanced only)
- Ability to have hosts, and ranges as well as subnets for destination networks
- Ability to allow local networks to obtain IP address using DHCP through the VPN Tunnel
- Ability to select user groups as well as users for inbound and outbound authentication on the VPN Tunnel (Enhanced only)
- Ability to apply NAT policies, which allow you to select the local and remote translated networks (Enhanced only)
- Ability to enable or disable management and user login on a per SA basis (Enhanced only)
- Ability to bind SA to a specific Zone (Enhanced only)
- VPN bandwidth management has been moved to access rules and is now on a per SA (rule) basis (Enhanced only)
- Fragmented packet handling has been moved to access rules and is now on a per SA (rule) basis (Enhanced only)

- Ability to restricted traffic on an SA-by-SA basis has been added. It allows restriction based on services, schedule, and specific users or groups (Enhanced only)

What VPN settings are simplified or are done automatically?

Note the following:

- A single field defines the SA lifetime for Phase One and Phase Two in 6.6.0.1 and older firmware; the maximum SA lifetime for a SonicWALL is 9,999,999 seconds, and the minimum SA lifetime is 120 seconds. This number was verified by engineering – older manuals and docs regarding SA lifetime may be incorrect (they state 2,500,000 as the max)
- SonicWALL's use time-based SA lifetimes and not data-based SA lifetimes, as some other Firewall/VPN vendors have implemented
- The lifetime negotiation may differ depending on the value the remote peer gateway proposes. If the lifetime proposed by the remote peer gateway is lower than what the SonicWALL SA is set to, the SonicWALL will negotiate the VPN tunnel with the lower of the two values
- IKE Identity is automatically set depending upon the mode in 6.6.0.1 and SonicOS 2.0.0.9 Standard. Enhanced firmware gives the user the option of setting the IKE Identity. Please refer to the next page for a full explanation of this topic
- SonicWALL Firmware 6.6 and SonicOS 2.0.0.9 Standard do not have a configuration option for local phase Two ID type -- it will always be 'subnet'. The peer VPN gateway must therefore be configured to always use a subnet ID for the SonicWALL endpoints, even if for a single host behind the SonicWALL. SonicOS 2.0.1.5 Enhanced allows the user to choose between hosts, ranges, and subnets
- Using "Apply NAT & Firewall rules" will make both 6.3.X & 6.4.X send the SonicWALL's WAN IP address with a 32-bit subnet mask as Phase 2 ID for the SonicWALL device
- As IKE Responder, SonicWALL can accept Diffie-Hellman 1, 2, or 5 (DH1, DH2, and DH5) - this is critical to remember when setting up a tunnel with a third-party device
- SonicWALLs support only 'tunnel' mode and not 'transport' mode for site-to-site VPN connections - 'tunnel' mode is used for both ESP and for AH – although 'transport' mode is used for L2TP client connections
- Replay Detection is automatically on for all IPSec traffic that uses IKE. Each IPSec packet has a Sequence Number that increases monotonically. The SonicWALL keeps a counter on IPSec packets on VPN tunnels and if it detects a packet that it has seen before, it is discarded. When a replayed packet is detected, the following message will appear in the log: "IPSEC Replay Detected". If attacks are checked under the 'Alerts' section in the log settings page, an email will be sent to the administrator, and the administrator should get a SNMP Trap. The SonicWALL will not do anything besides discarding the packet and incrementing an error counter that is usable or debugging
- In firmware 6.2.0.0 and older, the mode (Aggressive or Main) is automatically negotiated by the SonicWALL device during a VPN tunnel negotiation, depending on whether the peer gateway is explicitly specified or is absent (will negotiate in Aggressive if absent)
- In firmware 6.3.0.0 and newer, the administrator can explicitly set the mode (Aggressive or Main) for each SA

How does the SonicWALL handle IKE Identities?

Note the following:

Firmware 6.6

- In Aggressive Mode the device sends ID_USER_FQDN as its Phase One ID, and accepts ID_USER_FQDN or ID_FQDN from the remote peer gateway
- In Main Mode the device sends ID_IPv4_ADDR as its Phase One ID, and accepts ID_IPv4_ADDR from the remote peer gateway

SonicOS 2.x Standard

- In Aggressive Mode the device sends ID_USER_FQDN as its Phase One ID, and accepts ID_USER_FQDN or ID_FQDN from the remote peer gateway
- In Main Mode the device sends ID_IPv4_ADDR as its Phase One ID, and accepts ID_IPv4_ADDR from the remote peer gateway

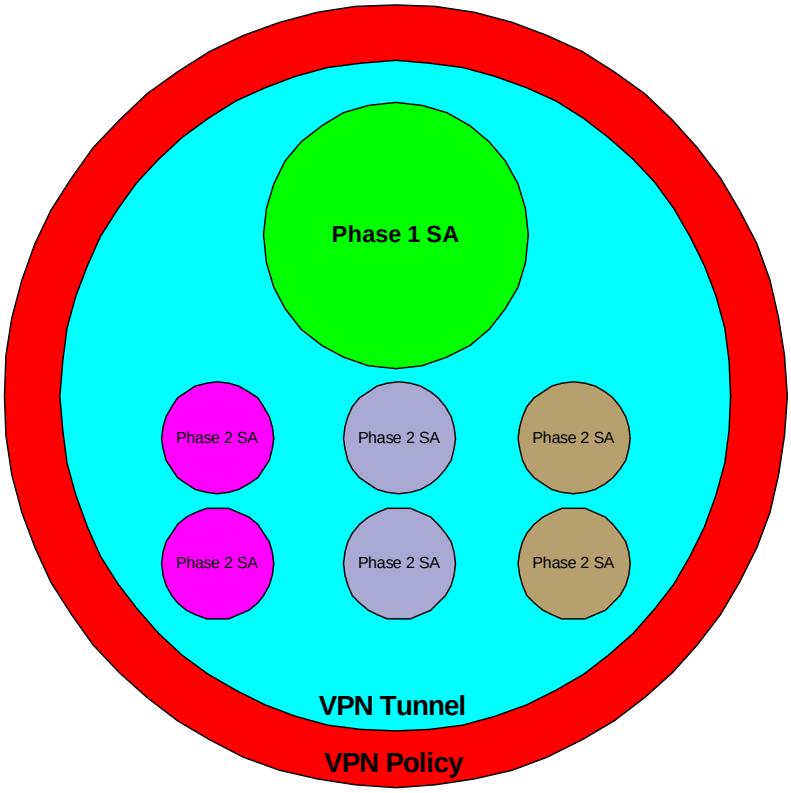
SonicOS 2.x Enhanced

- In Aggressive Mode with a site-to-site tunnel to another SonicWALL device **not** running Enhanced firmware, The Local IKE ID must be set to type SonicWALL Identifier (which is ID_USER_FQDN) and its value must be same as the SA "Name" field on the SonicWALL device not running enhanced firmware. The Remote IKE ID must be set to type SonicWALL Identifier and its value needs to be the same as the "Unique Firewall Identifier" of the SonicWALL device not running Enhanced
- In Aggressive Mode with a site-to-site tunnel to another SonicWALL device running Enhanced firmware, the user must configure the Local IKE ID and the Remote IKE ID. The user can pick from the following, IP Address, Domain Name, Email Address, and SonicWALL Identifier. The Local IKE ID on system one must be the same type and have the same value as the Remote IKE ID on system two and visa versa
- In Main Mode, if the user has not set Local IKE ID or Remote IKE ID, which should be the case unless this is a site-to-site setup with another device running Enhanced firmware, the device sends ID_IPv4_ADDR as it's Phase One ID, and expects ID_IPv4_ADDR from the remote peer gateway
- In Main Mode, and creating a site-to-site tunnel with another device running Enhanced firmware, the user can configure the Local IKE ID and the Remote IKE ID. The user can pick from the following, IP Address, Domain Name, Email Address, and SonicWALL Identifier. The Local IKE ID on system one must be the same type and have the same value as the Remote IKE ID on system two and visa versa

How many VPN tunnels can a SonicWALL device really handle?

First off, it's important to understand that there are differences between the definitions of what a VPN tunnel is, what a Security Association (SA) is, and what a VPN policy is. SonicWALLs are licensed for VPN policies – which is a singular connection a unique remote peer gateway. For example, the TZ170-U device is licensed for ten VPN policies, which means that it is capable setting up VPN connections with up to ten unique remote peer gateways. In some of our older documentation, SonicWALL used the generic term "VPN Tunnel", or referred to them as "profiles", which can be somewhat misleading. While "profiles" and "VPN policies" refer to the same thing, it's extremely important to note that a "VPN tunnel" or "SA" should not be considered the same. Remember that with IKE IPSec, at least three SA's are negotiated for each VPN tunnel – one phase one SA, and two unidirectional phase two SA's for each remote subnet. So on a TZ170-U, if you were to set up VPN tunnels to five unique remote peer gateways, and each had one remote subnet defined, you're actually talking about 15 SA's – and it would work fine.

The following example is useful to visualize the relationships:



It gets a little more complex when you start adding lots of remote subnets to each VPN policy, as the SonicWALL has a shared memory pool, and other functions on the device may utilize this pool. This means that if the device has other functions active (for example: AV, CFS, extensive firewall policy entries, IPS), it may adversely affect your ability to set up new VPN policies or add additional subnets to existing VPN policies -- even if the device is licensed for a specified number of policies. When our older documentation discusses how many “VPN Tunnels” or “profiles” each model can support, the number is really a best-case scenario, i.e. each VPN policy only has one remote subnet defined, the device does not have that many rules, AV and CFS/CFL are not enabled, etc.

How many IP subnets can you define for a VPN policy?

There is no enforced limit. However, this does not mean that there are not inherent limitations -- it gets a little more complex when you start adding lots of IP subnets, as the SonicWALL has a shared memory pool, and other functions on the device may utilize this pool. Please note that individual hosts, when specified explicitly as a destination network, are considered /32 subnets, and members of ranges are each considered a separate destination network.

Can I set up VPN tunnels using third-party certificates?
Yes. As of firmware 6.3.0.0, we support Verisign, Thawte, Baltimore, RSA Keon, Entrust, and Microsoft CA certificates for VPN tunnels from SonicWALL-to-SonicWALL. They are not supported for VPN tunnels between a SonicWALL device and the SafeNet VPN Client (any version), or a VPN tunnel between a SonicWALL device and a third-party VPN device (Check Point, Netscreen, Cisco, etc).

Can I use the built-in Windows XP IKE/IPSec client to make a VPN connection to a SonicWALL device?
Yes, but the setup & configuration on the Windows XP system is fairly complex and is not a trivial task. SonicWALL does not provide any technotes on its setup; users wishing to use the built-in IKE/IPSec client in Windows XP will need to contact Microsoft. SonicWALL strongly recommends using the SonicWALL Global VPN Client instead, since it's designed to work seamlessly with SonicWALL Firewall/VPN devices, and is incredibly easy to install, configure, and use.

Should I always use 3DES? What about DES? Or AES?
That depends – if it is crucial that the data never be compromised, and the performance impact is not an issue, and both sides can support it, then AES-256 is the way to go. Security administrators by nature are paranoid (which you can argue is what they're paid to be!) and generally will want to use the most secure mechanisms possible for a VPN setup: AES-256, Phase One DH5, SHA-1, Phase Two PFS-DH5, replay detection, short SA lifetime. As for DES, most security administrators no longer consider it secure, as it has been publicly demonstrated that it is susceptible to brute-force attacks given enough computing horsepower. For this reason, the FreeS/WAN project refused to even implement DES

What is ARCFour?
If you are setting up SonicWALL-to-SonicWALL VPN tunnels using GEN2 or earlier devices (TELE2, SOHO2, PRO/PRO-VX), you may wish to consider using ARCFour, since it is an extremely fast method of encryption and is not susceptible to any known attack. The drawback to ARCFour is that no other known vendor supports it as an encryption method for IPSec VPNs, and that it is not supported in any version of SonicOS.

Do all SonicWALLs support AES/Rijndael for IPSec VPNs?
No. AES is supported in all versions of SonicOS Enhanced and all versions of SonicOS Standard. AES is supported on the following platforms for Firmware 6.6: PRO100, PRO200, PRO230, PRO300, PRO330, GX2500, GX6500, all SOHO3-based, all TELE3-based, and the SOHO TZW.

Should I always use SHA-1? What about MD5?
There was a demonstrated attack against an older implementation of MD5, but the version that SonicWALL implemented its IKE/IPSec code is considered secure. MD5 is a 128-bit hash, while SHA-1 is a 160-bit hash. Using SHA-1 will result in a noticeable reduction in throughput. Use SHA-1 if the security policy dictates that the maximum level of protection be used whenever possible. If not, use MD5.

My SonicWALL device doesn't have SHA-1 or PFS. Why?
SHA-1 and PFS were not implemented until firmware 6.0.0.0 and newer. If you require either of those features, you will need to upgrade your SonicWALL's firmware to a version newer than 6.0.0.0. If you have an older SonicWALL (like an original TELE or SOHO device), using SHA-1 or PFS will not be possible, as they only support up to firmware 5.1.7.

Who has SonicWALL demonstrated IKE IPSec compatibility with?
SonicWALL has verified compatibility with these vendors' products:

- Cisco IOS IPSec Feature Set version 12.1.5T and newer
- Cisco PIX version 5.3.1 and newer
- Cisco 3000 VPN Concentrator version 3.0 and newer
- Cisco 5000 VPN concentrator
- NetScreen 5/10/100/500/1000 version 2.0.1 and newer
- Nortel Contivity version 04_06_120
- Checkpoint Firewall-1 version 4.0 and newer
- Checkpoint NG on NT FP3
- Checkpoint NG on Nokia 3Rs4
- Watchguard SOHO 2.3 and newer
- Watchguard Firebox 6.x and newer
- Alcatel PermitGate 2500/4500 version 2.1 and newer
- Symantec Raptor version 6.5 and newer
- Symantec Firewall/VPN Gateway version 1.5 and newer
- NAI Gauntlet version 5.5 and newer

PLEASE NOTE: untested peers should work as long as they abide by RFC's 2407, 2408, and 2409.

Where can I find technotes on how to set up VPN tunnels to third-party VPN devices?
All interop technotes can be found here: http://www.sonicwall.com/services/VPN_documentation.html -- towards the bottom of the page. These docs are written and maintained by members of SonicWALL's Architecture & Publications Group and are added/revised on a periodic basis.

Are there any known issues with VPN third-party interoperability?
SonicWALL-to-Check Point seems to be more troublesome than most, but that's mostly due to issues with Check Point's IPSec implementation. Check Point also tends to make changes to their IPSec implementation every time they release a service pack -- you can almost count on SonicWALL-to-Check Point tunnels not working after you apply one. SonicWALL-to-Cisco 3000 VPN Concentrator (a.k.a. the Altiga) has been one of the more troublesome pairings, but the problem can be addressed by upgrading the firmware to 3.5 or newer on the Cisco device, and 6.5.0.0 or newer on the SonicWALL device.

What is the VPN throughput of a SonicWALL?
All tests were done using the following parameters a 1496 byte packet, DES encryption, NAT Enabled. Please note that tests were conducted with UDP traffic, and that TCP, smaller packet sizes, or large packets requiring fragmentation will result in reduced throughput.

- GEN3 (TELE3/SOHO3) (running 6.1.X.X): 3.95 Mbps
- TZ170 (running 2.0.0.1S): 48.65 Mbps unidirectional, 24.35 Mbps bidirectional
- PRO 3060/4060 (running 2.0.0.1E): 96.77 Mbps unidirectional, 90.27 Mbps bidirectional

What good does "enabling NetBIOS broadcasts" do?
If both sides of the VPN tunnel are SonicWALL devices, it can greatly reduce the number of problems associated with Microsoft workgroup/domain networks, as the SonicWALL devices will forward all NetBIOS-Over-IP packets sent to the local LAN subnet's broadcast address across the VPN tunnel(s). Microsoft networking, unless explicitly configured otherwise, is heavily dependent upon local LAN broadcast messages; normally, edge devices such as routers, firewalls, or VPN devices discard these broadcast messages. Please note that this is a SonicWALL-only feature – do not activate it if the remote peer gateway for a VPN tunnel is not a SonicWALL device. It also is not currently supported for client VPN connections to SonicWALL's Global VPN Client, or Global Security Client.

What does the 'Enable Fragmented Packet Handling' checkbox do?
There are times at which the IKE IPSec traffic will be fragmented in transit. By default in 6.6.0.1 and SonicOS 2.0.0.9 Standard firmware, this checkbox is disabled, and because of this, fragmented IKE IPSec packets would be dropped. In SonicOS 2.0.1.5 Enhanced, the checkbox is enabled by default and it can be set on an SA by SA basis.

How important is the 'Deed Peer Detection' feature?
When IPSec was defined as a standard, they neglected to make recommendations for a common method to determine if an SA was still valid or not. When two sides perform IKE IPSec setup, they negotiate a Phase One SA, and then negotiate two or more Phase Two SA's for the traffic; all of these SA's (and the keys associated) have a pre-set lifetime. During the lifetime, both sides generally assume the SA's and keys are valid, and they do any sort of validity checking. If either side crashes or reboots, the other side has no way to determine that the SA is no good anymore, and will continue to keep sending traffic using that SA across it until the lifetime expires. Since the other side no longer has that SA -- remember, it either crashed or rebooted, so its been flushed -- it will reject the traffic. The other side will have to also be rebooted to get it working, or you will need to initiate traffic from the side that crashed/rebooted, since that will cause a totally new SA to be built. HOWEVER: as of 6.1.1.0 firmware, there's now a 'SA Keep Alive' checkbox in the 'Advanced' tab. Using this will cause the SonicWALL to perform validity checks on the SA's, and to automatically renegotiate any SA whose peer does not respond to the check (basically a very small heartbeat packet). Other vendors have had to implement similar proprietary mechanisms.

What version of DPD (Dead Peer Detection) is SonicWALL using?
The DPD mechanism we use in 6.6.0.1, SonicOS 2.0.0.9 Standard, and SonicOS 2.0.1.5 Enhanced is proprietary. RFC 3706 (DPD-Draft 4) will be implemented in SonicOS 2.5.

What's the difference between 'Dead Peer Detection' and 'SA Keepalive'?

Note the following:

Dead Peer Detection

The goal of this feature is to detect if our peer still has a valid IKE SA. If we have a tunnel established with a peer and the peer shuts down/reboots without notifying us, we will still try to use the older SA. To avoid this problem we added a proprietary dead-peer-detection mechanism. This is the same mechanism used by SafeNet VPN clients. Periodically, we send an 'IKE NOTIFY:KEEP-ALIVE-REQUEST' packet to the peer. If the peer also supports this mechanism, it will reply with an 'IKE NOTIFY:KEEP-ALIVE-RESPONSE' packet. These packets are encrypted & protected with Phase One SA (similar to quick mode messages). The peer can decrypt it correctly only if it still has the matching keys negotiated during Phase One. This feature will work only with consenting parties. i.e. SonicWALL firmware 6.1.x or newer and the SafeNet VPN client version 8.0 or newer. This mechanism is not really a heartbeat. We are not broadcasting "I-Am-Alive" messages -- instead we are periodically "pinging" the other end to see if it is alive. Please note that this feature will force an ISDN dial-on-demand line to dial out. Remember that the SonicWALL is sending these 'IKE NOTIFY:KEEP-ALIVE-REQUEST' messages every minute. These packets (IKE UDP port 500) will cause the line to activate.

KeepAlive

The goal of this feature is to keep a VPN tunnel always up with the other VPN endpoint. If this feature is enabled, we periodically check to see if a tunnel exists (Phase Two SA exists) with the other end. If a tunnel is not found a new negotiation is started (will start an outbound IKE negotiation - UDP 500 packet). This means that the tunnel will be established even when there is no network traffic to the other end. We check every 5 minutes to see if we have an IPSec SA (Phase Two SA) with the other end. This feature in itself does not send any extra packets. This feature can operate without Dead Peer Detection but will operate best in conjunction with Dead Peer Detection. Please note that this feature will also force an ISDN line to dial out, as noted above. There have been a few changes with the introduction of SonicOS Enhanced firmware -- we no longer periodically check for valid Phase 2 SA's. Instead, we trap all tunnel teardown & failure conditions and initiate a new negotiation if "Keep Alive" is turned on.

What does the 'NAT Traversal' checkbox do?

NAT Traversal checks to see if network address translation (NAT) is being performed between the two VPN tunnel endpoints, since this "in-between" NAT can interfere with VPN tunnel traffic. If NAT is indeed being performed those two endpoints, and both endpoints are capable of performing NAT Traversal, the VPN tunnel traffic will be encapsulated within UDP packets. Encapsulating the VPN traffic in UDP packets allows the VPN tunnel to be NAT'ed in between the endpoints. This feature was added in firmware 6.3.x.x, and is also supported in the 8.0 VPN Client. SonicWALL's implementation of NAT Traversal is based upon Draft 1('draft-ietf-ipsec-nat-t-ike-01.txt' and 'draft-ietf-ipsec-udp-encaps-01.txt').

How it works:

NAT Traversal is achieved by sending the NAT Traversal Vendor ID field in the first two messages in the Main Mode and Aggressive Modes. A MD5 Hash (draft-ietf-ipsec-nat-t-ike-00) is sent as Vendor ID hash. Upon the receipt of this Vendor ID, both sides can decide whether the other end supports NAT Traversal or not. A new payload called "NAT-Discovery" payload is sent in the message 2 and 3 in Main Mode, and message 2 and message 3 in the Aggressive Mode. The HASH function negotiated in the IKE is used in the HASH calculation. It can be MD5 or SHA. After receiving the NATD payload the IPSec Tunnel endpoints can determine whether a NAT device is in between by computing the HASH values locally and comparing with the HASH values

received. If a NAT device is detected in between the endpoints, in the phase 2 Quick mode instead of ESP Attribute, UDP_TUNNEL_ESP ->61443 or UDP_TRANSPORT_ESP ->61444 is sent depending on Tunnel/Transport mode. If a NAT device is not detected then there is no change in the Quick Mode. Once the IPSEC SA is negotiated in the Quick Mode, the ESP packets should be encapsulated in the UDP packets. The UDP encapsulation should use the same source and destination port as used in the IKE negotiations. The UDP encapsulation should be done only when a NAT device is present in between the endpoints. The Phase One initiator will send the keepalives. The keepalive is just to keep up the NAPT mapping with the NAT device in between.

What version of NAT-T is SonicWALL using?
SonicWALL currently implements the NAT_Tv00 draft in the following firmware: 6.6.0.1, SonicOS 2.0.0.9 Standard, and SonicOS 2.0.1.5 Enhanced. Additionally, the NAT_Tv03 draft is implemented in SonicOS 2.1.x.x and newer.

What exactly does the built-in 'GroupVPN' SA do?
The 'GroupVPN' SA in firmware versions 6.6.0.1, SonicOS 2.x.x.x Standard and Enhanced has four major differences. The 'GroupVPN' is hard coded to accept incoming connections from any peer gateway (in this case, the peer gateways are VPN Clients). The 'GroupVPN' doesn't have an 'add network' capability - instead it accepts the IP subnets that are directly attached to the interface the GroupVPN terminates on and/or any static routes on the LAN and/or additional LAN subnets defined. These subnets are used as the phase two networks to negotiate. The 'GroupVPN' is also hard coded to Aggressive Mode, and cannot be changed. And, the 'GroupVPN' has the 'Export Settings' button that takes all the settings and crunches them into a SPD file, compatible with the SafeNet IRE 5.x/8.x/9.x/10.x client. The 'GroupVPN' SA cannot be deleted – only disabled (by default, it is disabled). It is also interesting to note that the 'GroupVPN' connector accepts ID_USER_FQDN, ID_FQDN or IP_V4_ADDR as the remote gateway (client) IKE Identity, but it doesn't actually validate the value – it just accepts it.

<u>SonicOS 2.x.x.x Enhanced adds more flexibility to the GroupVPN SA:</u>

- Ability to specify destination networks on a per user and/or User Group basis.
- Apply firewall rules for VPN traffic on a per user and/or User Group basis.
- Added the ability to use this gateway itself to route all Internet traffic from VPN Clients instead of a separate gateway on the LAN.
- Complete DMZ network range is now parsed and automatically consolidated if necessary and then downloaded to the VPN client.
- When XAUTH is not enabled, extended functionality to allow unauthenticated users access to specific destination networks.

Can I create multiple VPN policies to the same remote peer?
No, at this time, no version of firmware supports this feature, but will be added in a future version of firmware to comply with ICSA 1.0D requirements.

What VPN clients can I use?
The listed versions of firmware 6.6.0.1, SonicOS 2.0.0.9 Standard, and SonicOS 2.0.1.5 Enhanced have been tested and are compatible with SonicWALL's Global VPN Client 1.x/2.x, IRE's SafeNet Client 8.x/9.x/10.x, The built-in IKE/IPSec connector in Windows XP, and Equinox's 'VPN Tracker' for Apple Macintosh systems (setup papers can be found here: http://www.equinux.com/us/products/vpntracker/interoperability.html).

What is the Unique Firewall Identifier (UFI)?
SonicWALL devices use this entry as their default IKE Identity when negotiating Aggressive Mode VPN tunnels. The entry, which can be found on the main VPN GUI page of all SonicWALL devices, defaults to the SonicWALL's MAC address, but can be customized to any value. The IKE Identity type for this field is ID_USER_FQDN.

What is 'VPN single-armed' mode?
This feature allows a SonicWALL device running firmware 6.6 or SonicOS 2.0 Standard to act as a stand-alone VPN gateway, with the WAN port utilized as a VPN tunnel termination point. Clear text traffic is statically routed to the WAN interface via internal routing process, and the data is encapsulated to the appropriate IPSec remote peer gateway. If 'VPN Single-Armed Mode (stand-alone VPN gateway)' is enabled, a dialog box appears with the following message: Selecting "VPN Single Armed mode", and will make this device accessible only from the WAN interface. This option will modify the intranet mode and add a HTTPS rule. Please note that this feature only works if the SonicWALL is in Transparent mode.

What is 'DHCP over VPN' and how does it work?
This feature is supported in Firmware 6.4 and above, and all versions of SonicOS. It allows remote SonicWALL devices to forward all LAN-side or DMZ/OPT-side DHCP requests off to a remote DHCP server located on the other side of a VPN tunnel, instead of using the SonicWALL's internal DHCP server. The feature is popular in hub-and-spoke environments where administrators want to issue all DHCP leases from a centralized source, regardless of whether the requesting clients are local or remote users. By using this feature, all scopes can be created, controlled, and monitored from a central location, instead of having to set up unique scope info on each remote SonicWALL device.

Can SonicWALL devices accept L2TP connections?
Yes – all versions of SonicOS 1.x and 2.x have a built-in L2TP-over-IPSec server that can terminate incoming L2TP connections. This feature is not supported in any 6.x firmware release, or any of the older firmware releases.

Can I terminate VPN tunnels on any interface?
In current versions of Firmware 6.6, SonicOS Standard, and SonicOS Enhanced, VPN tunnels actually terminate on the LAN interface, even though the remote peer may have been specified as the WAN or WLAN interface. In SonicOS 2.5 Enhanced, it will be possible to terminate VPN tunnels on any interface, for incoming Global VPN Client connections, as well as site-to-site VPN tunnels.

What does the 'Forward Packets to Remote VPNs' feature do in firmware 6.6 and SonicOS Standard?
This feature can be used to set up "hub-and-spoke" VPN networks, where the administrator wishes to allow all the remote sites to access each other, through the central site. This feature eliminates the need to set up a full-mesh VPN environment. This feature is enabled on all SA's on the central site that need to communicate with each other; on each remote site, it will be necessary to list all the central and remote peer destination networks in the VPN policy leading to the central site, in order for each remote site to connect to the other remote sites.

What do the 'VPN Terminated at' radio buttons do in firmware 6.6 and SonicOS Standard?
In these two firmware releases, it's not possible to manually specify which internal networks the SonicWALL will exchange during VPN negotiation. By default, the SonicWALL will only propose LAN-side subnets during VPN negotiation – this includes any secondary networks bound to the LAN interface, as well as any static IP routes set on the LAN interface. The radio buttons can be set to 'LAN', 'OPT' (in the TZW's case, 'WLAN'), or 'LAN/OPT'. Selecting the latter option will cause the SonicWALL to propose all known internal subnets during VPN negotiation.

Does the SonicWALL support XAUTH?
Yes, it does, and incoming users can be authenticated against the internal user database of the SonicWALL or an against external RADIUS servers. Future versions of SonicOS will be able to natively query Microsoft Active Directory servers and LDAP servers for user/password authentication for incoming VPN or ULA sessions. Please note that Microsoft Windows 2000 Server and Microsoft Windows 2003 Server come with a free RADIUS snap-in that allows external devices (such as a SonicWALL) to query Active Directory for usernames/passwords using RADIUS.

Can I force users to authenticate before accessing a site-to-site VPN tunnel?
Yes, this is possible if using firmware 6.4 or above, or any version of SonicOS. Authentication can be enforced in either direction of the tunnel, and the usernames/passwords can be polled either from the internal database on the SonicWALL device, or passed onto external RADIUS servers. If this feature is activated, the user must first navigate to the SonicWALL's LAN IP address using a web browser and successfully authenticate, before their traffic is allowed across the tunnel. This feature is particularly useful in home-office environments where the primary user requires access across a VPN tunnel to his or her corporate office, but there are other people also utilizing the home-office connection for public Internet connectivity that should not be allowed access to corporate resources across the tunnel. Using authentication on VPN tunnels solves this problem.

Can I set up a secondary VPN gateway for redundancy purposes?
Yes, this feature is available in firmware 6.6 and above, and SonicOS 2.0 and above. The feature allows a remote "spoke" device, such as a SonicWALL TZ 170, to utilize a primary remote peer as its main VPN gateway. The remote SonicWALL device uses Dead Peer Detection and Keepalives to check the status of the primary remote peer; if the primary remote peer stops responding, the remote SonicWALL device will renegotiate the VPN tunnel with the secondary remote peer – this may be another SonicWALL device entirely, or it may even be the secondary WAN port of the primary remote peer.

Do SonicWALL devices support IKEv2?
SonicWALL is currently working on this for a future version of SonicOS, with no ETA for delivery at present.

Created: 06/05/2002
Updated: 04/16/2004
Version 1.6