e quinux VPN Tracker for Mac OS X



How-to:

Interoperability with

SonicWALL

Internet Security Appliances

Rev. 3.1

Copyright © 2003-2004 equinux USA Inc. All rights reserved.

1. Introduction

This document describes how VPN Tracker can be used to establish a connection between a Macintosh running Mac OS X and a SonicWALL Internet Security Appliance.

The SonicWALL is configured as a router connecting a company LAN to the Internet.

This paper is only a supplement to, not a replacement for, the instructions that have been included with your SonicWALL. Please be sure to read those instructions and understand them before starting.

All trademarks, product names, company names, logos, screenshots displayed, cited or otherwise indicated on the How-to are the property of their respective owners.

EQUINUX SHALL HAVE ABSOLUTELY NO LIABILITY FOR ANY DIRECT OR INDIRECT, SPECIAL OR OTHER CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE USE OF THE HOW-TO OR ANY CHANGE TO THE ROUTER GENERALLY, INCLUDING WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS, OR DATA, EVEN IF EQUINUX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2. Prerequisites

First you have to make sure that your SonicWALL has VPN support built in. Please refer to your SonicWALL manual for details.

Furthermore you should use a recent SonicWALL fimware version. The latest firmware release for your SonicWALL appliance can be obtained from

https://www.mysonicwall.com/

For this document, 6.5.0.4 has been used.

When using Pre-shared key authentication you need one VPN Tracker Personal Edition license for each Mac connecting to the SonicWALL.

For certificate authentication you need a CA with private key, so one VPN Tracker Professional Edition is required in order to sign certificates. Only one VPN Tracker Professional Edition is required, other VPN users can use a Personal Edition. For further information please refer to chapter 3 in the VPN Tracker manual.

VPN Tracker is compatible with Mac OS X 10.2.x / 10.3.

In this example the Mac running VPN Tracker is directly connected to the Internet via a dialup or PPP connection.¹

The SonicWALL is configured in NAT mode and has the static WAN IP address 169.1.2.3 and the private LAN IP address 192.168.1.1. The Stations in the LAN behind the SonicWALL use 192.168.1.1 as their default gateway and should have a working Internet connection.



Figure 1: VPN Tracker – SonicWALL connection diagram

¹ Please note that the connection via a router, which uses Network Address Translation (NAT), only works if the NAT router supports "IPSEC passthrough". Please contact your router's manufacturer for details.

3.1 SonicWALL Configuration

The pre-defined VPN Tracker connection type has been created using the default settings for "Group-VPN". If you change any of the settings on the SonicWALL, you will eventually have to adjust the connection type in VPN Tracker.

Step 1 Change the Global VPN Settings:

- Enable VPN: checked
- Enable NAT Traversal: unchecked

000	SonicWALL Administration	0
SONICWALL	VPN	? Help
General	Summary Configure Authentication Service Local Certificates CA Certificates	
Log	Global VPN Settings	
Filter	Enable VPN	
Tools	Disable all VPN Windows Networking (NetBIOS) broadcast	
Access	Enable Fragmented Packet Handling	
Advanced	Keep Alive interval (seconds) 240	
DHCP	Dead Peer Detection Interval (seconds)	
VPN	Failure Trigger Level (missed heartbeats)	
Anti-Virus	VPN Bandwidth Management	
High Availability	Settings below will not take effect until enabled on Advanced Ethernet page. Enable VPN Bandwidth Management VPN guaranteed bandwidth 0.000 VPN maximum bandwidth 0.000 VPN bandwidth priority 0 highest \$	
	VPN Policies	
	Disabled Name Gateway Destinations Phase 2 Encryption/Authentication GroupVPN ESP DES HMAC MD5 (IKE) SAs enabled: 1 SAs defined: 1 SAs Allowed: 51	CZ Ū
	Currently Active VPN Tunnels	
	<u>Name Local Remote Gateway</u>	
		Update Reset
Logout	STATUS: The configuration has been updated.	1.

Figure 3: SonicWALL - Summary

Step 2 Change the GroupVPN Settings:

- Security Association: GroupVPN
- Phase 1 Encryption/Authentication: 3DES & SHA1
- Phase 2 Encryption/Authentication: "Strong Encrypt and Authenticate (ESP 3DES HMAC SHA1)"
- Shared Secret: your Pre-share key

000	SonicWALL Administration
SONICWALL	VPN 3 Help
General	Summary Configure Authentication Service Local Certificates CA Certificates
Log	Add/Modify IPSec Security Associations
Filter	Security Association GroupVPN
Tools	IPSec Keying Mode IKE using pre-shared secret 🔶
Access	Disable This SA 🗌
Advanced	Security policy
DHCP	Phase 1 DH Group Group 1 🜩
VPN	SA Life time (secs) 28800
Anti-Virus	Phase 1 Encryption/Authentication 3DES & SHA1 🗢
High Availability	Phase 2 Encryption/Authentication Strong Encrypt and Authenticate (ESP 3DES HMAC SHA1)
	Shared Secret yoursecretkey
	Advanced Settings
	Client Settings
	Export Settings
	Export Settings
Logout	STATUS: Ready

Figure 4: SonicWALL – Group VPN Configuration

Step 3 Change the Advanced settings:

• Default LAN Gateway: o.o.o.o

$\Theta \Theta \Theta$	VPN Advanced Settings	\bigcirc
Edit Advance	d Settings	
Note that afte	Require authentication of VPN clients via XAUTH: Enable Windows Networking (NetBIOS) broadcast Apply NAT and firewall rules Forward packets to remote VPNs Enable Perfect Forward Secrecy Phase 2 DH Group Group 1 ÷ Default LAN Gateway 0.0.0. VPN Terminated at • LAN ODMZ OLAN/DMZ OK Cance er clicking OK you must click Update on the main page to save changes made here.	

Figure 5: SonicWALL – Advanced Settings

Please note: In order to authenticate multiple clients with different credentials, please enable "Require Authentication of VPN Clients via XAUTH". In this case you'll also need to check "Extended Authentication (XAUTH)" in your VPN Tracker Authentication settings. Additionally you'll need to enable "Access from VPN client with XAUTH" for the specific user. Please refer to the SonicWALL manual for further assistance regarding user management.

3.2 VPN Tracker Configuration



- Vendor: "SonicWALL"
- Model: your VPN device

00	Connection: New York
	Connection: New York
Connec	tion Network Authentication Identifiers DNS
	Vendor: SonicWALL
Conne	Model: SonicWALL PRO 100 SonicWALL PRO 200 SonicWALL PRO 2040 SonicWALL PRO 230 Edit How-To ection Options: Initiate connection from this end Connect only when needed
Click the	lock to prevent further changes.

Figure 5: VPN Tracker - Connection settings

Step 2 Change your Network Settings:

- VPN Server Address: public IP address of your VPN Gateway (e.g. **169.1.2.3**)
- Remote Network/Mask: network address and netmask of the remote network (eg. 192.168.1.0/255.255.25.0).

$\bigcirc \bigcirc \bigcirc \bigcirc$	Con	nection: New York	
	Connection:	lew York	
Connecti	on Network	Authentication	Identifiers DNS
	Topology:	Host to Network	•
Ν	letwork Port:	Automatic	•
VPN Gate	way Address: 1	.69.1.2.3	
Lo	ocal Address:		optional
Remote Ne	twork/Mask: 1	.92.168.1.0 /	255.255.255.0 +
Click the lo	ck to prevent furt	ther changes.	Revert Save

Figure 6: VPN Tracker – Network settings

Please note: In order to access multiple remote networks simultaneously, just add them by pressing the Plus-button.²

² For this step VPN Tracker Professional Edition is needed.

Step 3 Change your Authentication Settings:

- Pre-shared key: the same Pre-shared key as in the SonicWALL configuration.
- Enable XAUTH if the corresponding option is enabled on the SonicWALL.

00	Connection: New York
Co	 Pre-shared key: presharedkey Hide typing Enter key when establishing connection The key will not be saved on disk.
£	Cancel OK Enable Extended Authentication (XAUTH)
Click	the lock to prevent further changes.

Figure 7: VPN Tracker - Authentication settings

Step 4 Change your Identifier Settings:

- Local Identifier: Local endpoint IP address.
- Remote Identifier: Remote endpoint IP address.

🖲 🖯 🔿 Ca	onnection: New York
Connection:	New York
Connection Networ	k Authentication Identifiers DNS
Local Identifier: Remote Identifier:	 Local endpoint IP address Own certificate Remote endpoint IP address Remote certificate Verify remote identifier
Click the lock to prevent f	urther changes.
	Revert Save

Figure 8: VPN Tracker - Identifier settings

Step 5 Save the connection and Click "Start IPsec" in the VPN Tracker main window.

You're done. After 10-20 seconds the red status indicator for the connection should change to green, which means you're securely connected to the SonicWALL. After IPsec has been started, you may quit VPN Tracker. The IPsec service will keep running.

Now to test your connection simply ping a host in the SonicWALL network from the dialed-in Mac in the "Terminal" utility:

ping 192.168.1.10

··· Troubleshooting

If the status indicator does not change to green please have a look at the log file on both sides. You can define the amount of information available in the log file in the VPN Tracker preferences. Below you can find a list of common error messages in the SonicWALL log file:

Log message: IKE Responder: IKE proposal does not match (Phase 1)

Log message: IKE Responder: Tunnel terminates inside firewall but proposed local network is not inside firewall

Solution: Check the Remote Network settings in VPN Tracker.

4. Connecting a VPN Tracker Host to a SonicWALL Firewall using Certificates

For Certificate Authentication, you'll need a CA with private key, so one VPN Tracker Professional Edition is required if you don't yet have a signing CA. Only one VPN Tracker Professional Edition is required, other VPN users can use a Personal Edition. For further information please refer to chapter 3 in the VPN Tracker manual.

4.1 <u>SonicWALL Configuration</u>

Step 1

Check "Enable VPN" and disable "NAT Traversal" and click "Update" when you are finished.

000	SonicWALL Administration	0
SONICWALL	VPN	? Help
General	Summary Configure Authentication Service Local Certificates CA Certificates	
Log	Global VPN Settings	
Filter	Enable VPN	
Tools	Disable all VPN Windows Networking (NetBIOS) broadcast	
Access	Enable Pragmented Packet Handling	
Advanced	Keep Alive interval (seconds) 240	
DHCP	Dead Peer Detection Interval (seconds)	
VPN	Failure Trigger Level (missed heartbeats)	
Anti-Virus	VPN Bandwidth Management	
High Availability	Settings below will not take effect until enabled on Advanced Ethernet page.	
	Canabic VPN Bandwidth Management VPN guaranteed bandwidth 000 VPN maximum bandwidth 000 VPN bandwidth priority 0 highest VPN bandwidth priority 0 highest VPN Policies Disabled Name Gateway Destinations Phase 2 Encryption/Authentication GroupVPN ESP DES HMAC MD5 (IKE) SAs enabled: 1 SAs enabled: 1 SAs defined: 1 SAs anabicd: 1 SAs anabicd: 1 SAs defined: 1 Sander Gateway	CY II
		Jpdate) Reset)
Logout	STATUS: The configuration has been updated.	1

Figure 9: SonicWALL - Global VPN Settings

Step 2 Please go to [VPN -> Local Certificate] and generate a "Certificate Signing Request". Enter a "Certificate name" and a "Common name" for the Certificate. You have to use a "Subject Alternative Name (Optional)". Select "Domain Name" and enter an arbitrary name. This setting refers to the "Remote Identifier" in VPN Tracker.

000	© Sonio	WALL Administration	C
SONICWALL General	VPN Summary Configure Authentication Se	rvice Local Certificates CA Certificates	• Help
Log	Current Certificates		
Filter	Certificates:	-Add New Local Certificate- 🖨	
	Import Certificate with private key		
Tools	Certificate Name:		
Access	Certificate Management Password:		
Advanced	Please select a file to import:	Durchsuchen	
DHCP		Import	
VPN	Generate Certificate Signing Request		
Anti Minun	Certificate Name:	sonicwall	
Anti-virus	Country	Us	
High Availability	State 🔶		
	Locality, City, or County 🗢		
	Company or Organization 🚖	equinux	
	Department 🔶		
	Group		
	Team 🔶		
	Common Name 🗢	sonicwall	
	Subject Distinguished Name:	C=US;O=equinux;CN=sonicwall	
	Subject Alternative News (Ontional)		
	Subject Alternative Name (Optional):	conicural	
	Subject Kay Tume:	DCA	
	Subject Key Size:	1024 hits	
	Subject Key Size.		
		Generate	
Logout	STATUS: Ready		

Figure 10: SonicWall - Certificate Signing Request

Step 3 Export the certificate request to a file, import the Request in the "Request" tab in VPN Tracker. Finally "Sign" the request with a CA. The "Alternative Name" field is predefined with the value you entered in the Certificate Signing request. It should be the same as the "Alternate Subject Name", defined before.

Sign Certificate
Settings
Signing CA: equinux Inc. CA
Validity: 365 days 🛟
Extensions
Alternative Name: DNS 🛟 sonicwall
Certificate Type: 📄 Client 📄 Email 📄 Server
Basic Constraints: 📃 Critical
Cancel Previous Next

Figure 11: VPN Tracker - Sign Certificate

Step 4 Export the signed certificate in the PEM- format and Import the Certificate in the SonicWALL.

Please note: The "Alternative subject name" of the certificate must be set and the Subject name Type must be "Domain Name".

After step 4 the configuration should look like this:

000	SonicWA	LL Administration	\odot
SONICWALL	VPN Summary Configure Authentication Service	Local Certificates CA Certificates	0 Help
	Current Certificates		
Log	Certificates:	sonicwall 🗢	
Filter	Certificate Details		
Tools	Certificate Authority:	/O=equinux AG/L=M\x9Fnchen/C=DE/Email=	
Access	Subject Dictinguished Name:	spang@equinux.com/CN=equinux Inc. CA	
Advanced	Certificate Issuer:	/O=equinux AG/L=M\x9Fnchen/C=DE/Email=	
DHCP		spang@equinux.com/CN=equinux Inc. CA	
VPN	Certificate Serial Number:	00	
	Expires On:	Jun 17 11:33:19 2004 GMT	
Anti-Virus	Alternate Subject Name:	sonicwall	
High Availability	Alternate Subject Name Type:	Domain Name Verified	
	Certificate Management Password	Delete This Certificate	
Logout	STATUS: Ready		1.

Figure 12: SonicWALL - Import the signed Certificate

Step 5 On the Sonicwall go to [VPN -> CA Certificates] and import the CA, which you used for signing, into the Sonicwall. The CA file must be exported in the DER- format.

000	SonicWALL Administration
SONICWALL	vpn 😯 Help
General	Summary Configure Authentication Service Local Certificates CA Certificates
Log	Certificate Details
Filter	Certificates equinux Inc. CA
Tools	
Access	Certificate Authority: /O=equinux AG/L=M\x9Fnchen/C=DE/Email=spang@equinux.com/ CN=equinux Inc. CA
Advanced	Subject Distinguished Name: /O=equinux AG/L=M\x9Fnchen/C=DE/Email=spang@equinux.com/
DHCP	Certificate Issuer: /O=equinux AG/L=M\x9Fnchen/C=DE/Email=spang@equinux.com/
VPN	CN=equinux Inc. CA Certificate Serial Number: 00
Anti-Virus	Expires On: Oct 16 11:19:02 2027 GMT
High Availability	No CRL loaded:
	Delete This Certificate Export This CA Certificate
	Please select a file to import Certificate Revocation List: Durchsuchen Import
	Enter CRL's location for this CA (URL):
Logout	STATUS: Ready

Figure 13: SonicWALL - Import your CA

Step 6 Please go to [VPN -> Configure] and configure the predefined Security Association "GroupVPN":

- IPSec Keying Mode: IKE using 3rd Party Certificates
- Select Certificate: select your previously imported Certificate
- Peer ID Type: Domain Name
- Peer ID Filter: Domain Name of the client certificate (e.g. vpntracker)

000	SonicWALL Administration	0				
SONICWALL	VPN	? Help				
General	Summary Configure Authentication Service Local Certificates CA Certificates					
Log	Add/Modify IPSec Security Associations					
Filter	Security Association GroupVPN					
Tools	IPSec Keying Mode IKE using 3rd Party Certificates					
Access	Select Certificate sonicwall 🗢					
Advanced	Disable This SA 🗌					
DHCP	Security policy					
VPN	Phase 1 DH Group 1					
Anti-Virus	SA Life time (secs) 28800					
High Availability	Phase 1 Encryption/Authentication 3DES & SHA1					
	Phase 2 Encryption/Authentication Strong Encrypt and Authenticate (ESP 3DES HMAC SHA1)					
	Prov Contificator					
	Peer ID Type: Domain Name					
	Peer ID Filter: vpntracker					
	Peer Certificate Must be Signed by Issuer of "sonicwall" Certificate					
	Advanced Settings					
	Client Settings					
	Export Settings					
	Upda	te Reset				
		Ų				
Logout	STATUS: Ready					

³ For this step, VPN Tracker Professional Edition is required.

4.2 VPN Tracker Configuration

Step 1 Create a new "Own certificate" for VPN Tracker.

Go to the VPN Tracker certificate manager (# + "E") and create and sign a new certificate. You have to use an "Alternative Name". Choose DNS from the drop-down box and enter the alternative name. This name must be the same as the "Peer ID Filter" field in your SonicWALL VPN settings.

Certificate Details						
X.509 Name						
Common Name:	vpntracker					
Organization:	equinux					
Organizational Unit:						
Locality (e.g. City):	Munich					
State or Province:						
Country:	DE					
Email Address:	vpntracker@equinux.net					
Settings						
Validity:	365 days 🛟					
Key Length: 1024						
Extensions						
Alternative Name:	DNS 🗘 vpntracker					
Certificate Type: 🗌 Client 📃 Email 🗌 Server						
Basic Constraints: 📃 Critical						
Cance	Previous Next					

Figure 15: VPN Tracker - Own certificate

⁴ For this step, VPN Tracker Professional Edition is required.

4. Connecting a VPN Tracker Host to a SonicWALL Firewall using Certificates

Step 2-3 Please refer to section 3.2 step 1-2.

Step 4 Change your Authentication Settings:

- Own Certificate: a self-signed certificate, created by VPN Tracker
- Remote Certificate: Verify with CA's

0	Connection: New York				
	Own Certificate: vpntracker				
	Edit Certificates Cancel OK				
Authenticate Using: O Pre-shared key Edit					
	Certificates Edit				
	Enable Extended Authentication (XAUTH)				
	Click the lock to prevent further changes.				
	(Revert Save)				
_					
1000					

Figure 17: VPN Tracker - Authentication Settings

Step 5 Change your Identifier Settings:

- Local Identifier: Domain Name of the self-signed certificate (e.g. vpntracker)
- Remote Identifier: Domain Name of the SonicWALL certificate (e.g. sonicwall)

(🖲 🖯 🔿 🔘	onnection: New York						
Connection:	New York						
Connection Networ	k Authentication	Identifiers	DNS				
Connection Network Autnentication Identifiers DNS Local Identifier: Local endpoint IP address Own certificate FQDN Remote Identifier: Remote endpoint IP address Remote certificate Image: Sonicwall FQDN Verify remote identifier Verify remote identifier							
Click the lock to prevent further changes.							
<u> </u>	C	Revert	Save				

Figure 18: VPN Tracker - Identifier Settings

Step 6 Please refer to section 3.2 step 5.