IP Office Technical Tip

Tip no: **190**

Release Date: **September 27, 2007**

Region: **GLOBAL**

Configuring a VPN Remote IP Phone with a Sonicwall Tz170 Standard / Enhanced VPN Router

The following document assumes that the user/installer is familiar with configuring both the IP Office and VPN devices as well as setting manually configuring IP hard phones. This document is for reference purposes only when creating the VPN tunnels and does not provide details on how to configure any other aspect of either device.

Test Systems Software Versions and Basic Phone Settings

IP Office Core Software	4.0.7
Sonicwall TZ170 Standard Mode	3.1.3.0-6s
Sonicwall VPN License	Yes
Sonicwall TZ170 Enhanced Mode	3.2.3.0-6e
IP Phone Model	5610
IP Phone Firmware	2.3.249
IP Office IP Address	192.168.2.5
TFTP/File Server	192.168.2.10
IP Phone IP Address	DHCP
IP Phone CallSV	192.168.2.5
IP Phone CallSVPort	1719 [Default]
IP Phone Router	DHCP
IP Phone Mask	DHCP
IP Phone FileSv	192.168.2.10
IP Phone 802.1Q	Auto
IP Phone VLAN ID	0
Password used during testing	1234567890
Remote ID used for Standard Mode test	GroupVPN
Remote ID used for Enhanced Mode test	GroupVPN

Notes

1. The IP Phones may require a Virtual IP Address to be configured in the VPN settings. Please take care in choosing a Virtual IP Range. Consider where the phone is most likely to be used and ensure that the Virtual IP Range selected will not conflict. For instance, many VPN IP Phones may be installed at user's homes. Typically a Home Router uses 192.168.0.x or 192.168.1.x as its internal network range therefore it is recommended that this is not used as a Virtual IP Address Range.

2. **IMPORTANT**: Many VPN Routers will not allow a direct media path to be established between two VPN Endpoints. It will be necessary to uncheck the Direct Media Path checkbox in the Extension Configuration in IP Office. Failure to do so will result in No Speech path when two VPN extensions try and establish a call.

3. Review the Sample 46vpnsetting.txt file for simplifying configuration settings on the IP Phones.

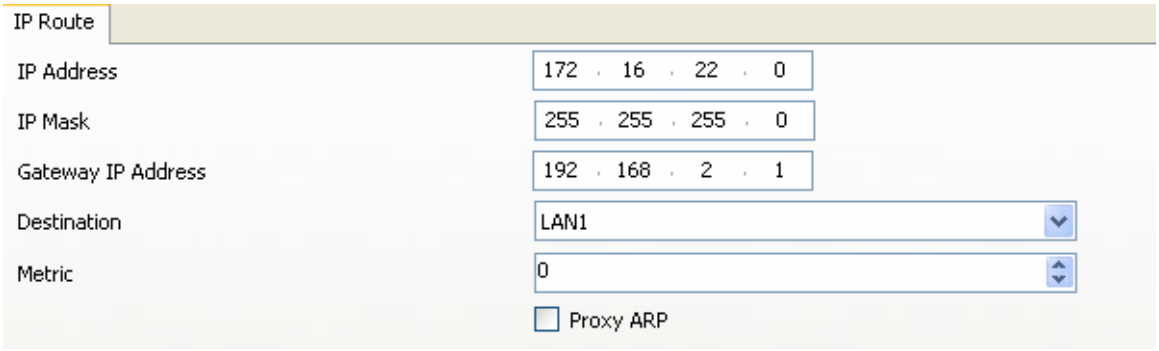
4. While the defaults for Encryption are set at 4500-4500 and these settings are preferred, there may be instances where (depending on what the Home router supports) the user may need to either disable this setting, or change to one of the other options.

5. If manually configuring a Virtual IP Address on the IP Hard-phone, ensure that accurate records are kept of IP Address allocations to avoid IP Address conflicts.

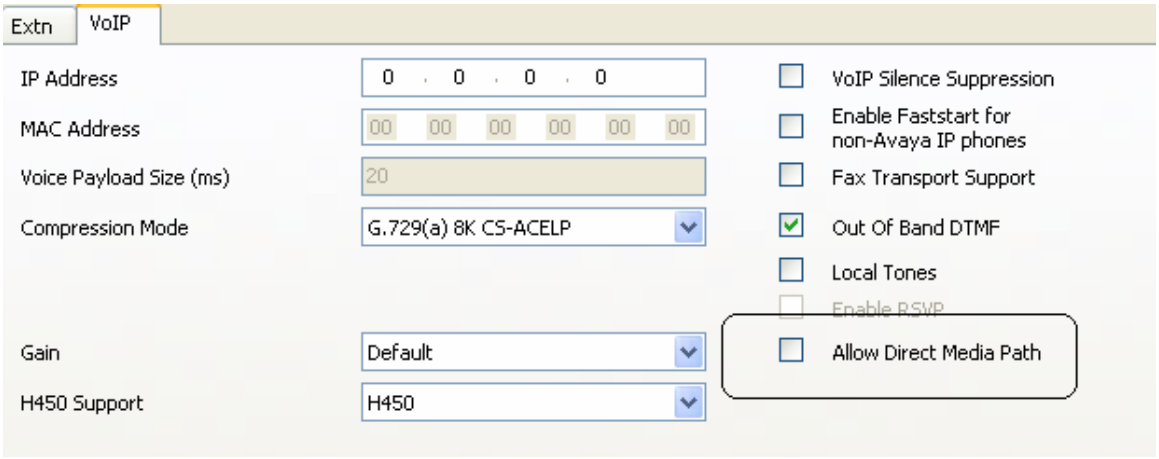
IP Office Configuration

Using IP Office Manager, Open the Configuration and Select IP Routes.

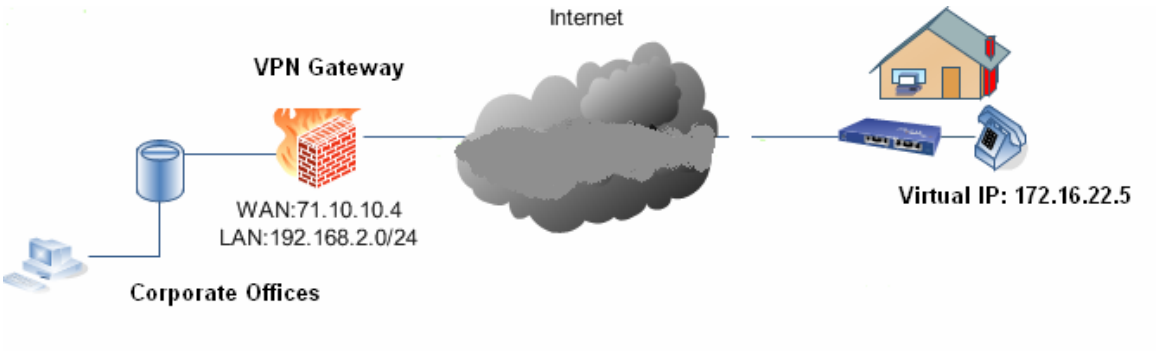
Add a New IP Route for the Virtual LAN Network to be used in the environment.



Modify the Extensions – VoIP Tab for those extensions that will be VPN Extensions, and uncheck the Direct Media Path Check Box.



Networking Scenario:



Sonicwall Tz170 VPN Router VPN Configuration settings

Important Note: Please note that the Sonicwall TZ170 Enhanced Mode has additional configuration options that need to be set. Please ensure that correct settings guidelines are followed.

Once logged into the Router, Select the VPN Option, then Select Settings

Global Settings	
Enable VPN	Checked
Unique Firewall Identifier	Default Firewall Identifier
VPN Policies	
GroupVPN (Standard)	Enable (Disabled by default)
WAN GroupVPN (Enhanced)	Enable (Disabled by default)

Select the Edit Icon to modify the VPN Policy

General Tab	
Security Policy	
IPSec Keying Mode	IKE using Preshared Secret
Name Standard	GroupVPN
Enhanced	WAN GroupVPN
Shared Secret	1234567890
Proposals Tab	
IKE (Phase 1) Proposal	
DH Group	2
Encryption	3Des
Authentication	SHA1
Life Time (seconds)	28800
IPSEC (Phase 2) Proposal	
Protocol	ESP
Encryption ALG	3DES
Authentication ALG	SHA1
Enable Perfect Forward Secrecy	Checked
DH Group	2
Life Time (seconds)	28800
Advanced Tab	
Advanced Settings	
Enable Windows Networking (Netbios) Broadcast	Unchecked
Apply NAT and Firewall Rules	Unchecked (Standard)
Forward packets to remote VPNs	Unchecked (Standard)
Management via this SA	HTTP/HTTPS – Unchecked (Enhanced)
Default Gateway	0.0.0.0
VPN Terminated at	LAN (Standard)
Client Authentication	
Require Authentication of VPN Clients via XAUTH	Unchecked
Allow Unauthenticated VPN Client Access	LAN Primary Subnet (Enhanced)
Client Tab	
User Name and Password Caching	
Cache XAUTH User name and password on Client	Never
Client Connections	
Virtual Adapter settings	DHCP Lease or Manual Configuration
Allow Connections to	Split Tunnels
Set Default Route as this Gateway	Unchecked
Require Global Security Client for this connection	Unchecked
Client Initial Provisioning	
Use Default Key for Simple Client Provisioning	Unchecked

Select the Advanced VPN Settings Page and ensure the following options are enabled (usually enabled by default)

Advanced VPN Settings	
Enable IKE Dead Peer Detection	Enabled
Dead Peer Detection Interval (seconds)	60
Failure Trigger Level (missed heartbeats)	3
Enable Fragmented Packet Handling	Enabed
Ignore DF (don't fragment) Bits	Enabled
Enable NAT Traversal	Enabled

Sonicwall: VPN Remote Phone Settings

VPN Remote Phone Configuration	
VPN Profile	Generic PSK
Server	71.10.10.4
IKE ID	GroupVPN (case sensitive)
PSK – (Pre Shared Key)	1234567890
IKE Parameters	
IKE ID Type	FQDN
Diffie Hellman Group	2
Encryption ALG	3Des
Authentication ALG	Sha1
IKE Xchange Mode	Aggressive
IKE Config Mode	Disabled
XAUTH	Disable
Cert Expiry Check	Disabled
Cert DN Check	Disabled
IPSEC Parameters	
Encryption ALG	3DES
Authentication ALG	Sha1
Diffie Hellman Group	2
VPN Start Mode	Boot
Password Type	Save in Flash
Encapsulation	4500 – 4500
Protected Nets	
Virtual IP	172.16.22.5
Remote Net #1	192.168.2.0/24
Remote Net #2	
Remote Net #3	
Copy TOS	No
Connectivity Check	Always
QTEST	Disabled

Issued by:
Avaya GSS Tier 4 Support
Contact details:-
EMEA/APAC
Tel: +44 1707 392200
Fax: +44 (0) 1707 376933
Email: gsstier4@avaya.com

NA/CALA
Tel: +1 732 852 1955
Fax: +1 732 852 1943
Email: IPOUST4ENG@Avaya.com

Internet: http://www.avaya.com