Avaya Secure Router 2330/4134

Advanced Gateway 2330

Avaya 96xx Series IP Phones

Engineering

> Secure Router IPsec with NAT-T Interoperability with Avaya 96xx IP Phones Technical Configuration Guide

Avaya Data Solutions

Document Date: December 2011

Document Number: NN48500-631

Document Version: 2.0

© 2011 Avaya Inc.
All Rights Reserved.

Notices
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http:// www.avaya.com/support.

Abstract

This document provides information on how to configure IPsec with NAT-T on the Avaya Secure Router 4134 and 2330 to interoperate with the IPsec client on the Avaya 96xx series IP Phones. This enables the Avaya 96xx phone to establish a secure IPsec tunnel to the Secure Router.

Revision Control

No	Date	Version	Revised By	Remarks
	11/14/2011	0.1	Jeff Cox	Initial Draft
	11/22/2011	0.2	Jeff Cox	Edits based on review feedback
	12/5/2011	1.0	Jeff Cox	Released version
	1/03/2012	2.0	Jeff Cox	Fixed error in SR Route Table Display

Table of Contents

1.1 Hardware 8
1.2 Network Topology 8
2.1 Secure Router 4134 10
2.1.1 Interface Configuration 10
2.1.2 IPsec Configuration 13
2.1.3 Firewall Configuration 14
2.2 9630 IP Phone 17
2.2.1 IPsec Configuration 17
2.3 Monitoring IPsec on SR4134 18

Figures

Figure 1 – Network Topology 9

Tables

Table 1 – Applicable Secure Router Platforms 8
Table 2 – IP Phone 9630 IPsec Parameters 18

Conventions

This section describes the text, image, and command conventions used in this document.

Symbols



Tip – Highlights a configuration or technical tip.



Note – Highlights important information to the reader.



Warning – Highlights important information about an action that may result in equipment damage, configuration or data loss.

Text

Bold text indicates emphasis.

Italic text in a Courier New font indicates text the user must enter or select in a menu item, button or command:

```
ERS5520-48T# show running-config
```

Output examples from Avaya devices are displayed in a Lucida Console font:

```
ERS5520-48T# show sys-info

Operation Mode:          Switch
MAC Address:             00-12-83-93-B0-00
PoE Module FW:           6370.4
Reset Count:             83
Last Reset Type:         Management Factory Reset
Power Status:            Primary Power
Autotopology:            Enabled
Pluggable Port 45:       None
Pluggable Port 46:       None
Pluggable Port 47:       None
Pluggable Port 48:       None
Base Unit Selection:     Non-base unit using rear-panel switch
sysDescr:                Ethernet Routing Switch 5520-48T-PWR
                         HW:02       FW:6.0.0.10  SW:v6.2.0.009
                         Mfg Date:12042004    HW Dev:H/W rev.02
```

1. Introduction

This technical configuration guide outlines the steps needed to configure a secure IPsec tunnel between the Avaya Secure Router 4134 and the Avaya 9630 series IP phone. This configuration allows customers to deploy Avaya 9600 series IP phones securely using IPsec Virtual Private Networking technology

This document applies to the following Avaya Secure Router and Avaya Advanced Gateway platforms:

Platform	Version	Tunnel Support
Secure Router 4134 with VPN Encryption Module	10.3	Up to 1000 Tunnels
Secure Router 2330 with VPN Encryption Module (SCIM)	10.3	Up to 100 Tunnels
Advanced Gateway with Secure Router Upgrade License and VPN Encryption Modules (SCIM)	10.3	Up to 100 Tunnels

Table 1 – Applicable Secure Router Platforms

1.1 Hardware

The following hardware and software were used to validate the configuration outlined in this technical configuration guide

- Secure Router 4134 version 10.3.2
- Avaya 9630 version 3.1
- Avaya S8710 running version R015x.02.1.016.4

1.2 Network Topology

Following is the network topology used to validate this technical configuration guide. The topology simulates a typical SOHO user that connects to the corporate network using an IPsec VPN tunnel. A Contivity 221 router was used as the SOHO router in this topology and is configured to use Port Address Translation (PAT) to translate the source IP address and source port numbers of packets sent from the 9630 IP phone. An IPsec tunnel is initiated on the 9630 IP phone and terminated on the SR 4134. Once the tunnel is established, the 9630 registers with the Avaya S8710 Media Server located on the corporate intranet. After registration, the SOHO user can communicate securely with anyone located inside or outside the corporate network.

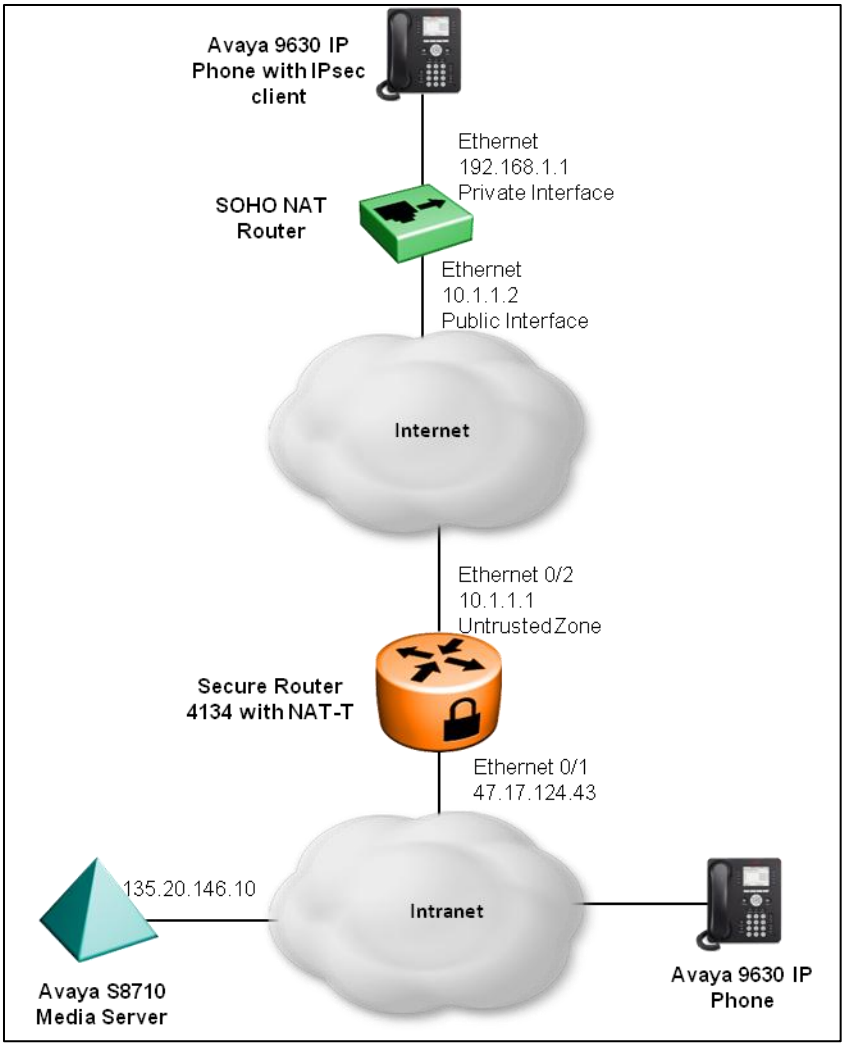


Figure 1 – Network Topology

2. Configuration

2.1 Secure Router 4134

This technical configuration guide assumes that the reader is familiar with the operation and configuration of the SR4134 and that the appropriate software version is loaded and operational.

The following are the configuration commands used to establish an IPsec tunnel to the 9630 IP Phone. You configure the 4134 by entering commands in “configuration mode” via the CLI. To enter this mode type, “configure terminal” from the operational mode prompt (#). Only the parameters applicable to setting up an IPsec tunnel are shown.

2.1.1 Interface Configuration

In this section, the public and private IP interfaces will be configured on the SR4134.

Before IPsec can be configured, you must verify the SR4134 has the VPN encryption module installed

1 Login to the CLI and verify the encryption module is installed.

```
SR# show chassis

Chassis Model: SR4134
Chassis Operational Status: NORMAL

Chassis Serial number: LBNNTMC94119L26032
Chassis Rev: 17
Slot/SubSlot    Card-Type       Status        Serial#
-------------------------------------------------------
   0            MPU_A           NORMAL        LBNNTMC97726L25119
   5            LMG_10          NORMAL        LBNNTMC99023L21030
   3            WTE_2M          NORMAL        LBNNTMC98108K36086
  INT           VPN_A           NORMAL        LBNNTMC98007L45139
  0/3           SFP             Absent        ---
  0/4           SFP             Absent        ---
  5/5           LMG_10 SFP      Absent        ---
  5/10          LMG_10 SFP      Absent        ---
```

VPN encryption module is installed and shown in red

2 Configure the public IP address on Ethernet interface 0/2.

```
SR# configure terminal
SR/configure# interface ethernet 0/2
SR/configure/interface/ethernet (0/2)# ip address 10.1.1.1 255.255.255.0
```

3 Add the public IP interface to the untrusted zone

```
SR/configure/interface/ethernet (0/2)# crypto untrusted
SR/configure/interface/ethernet (0/2)# exit
```

4 Configure the private IP address on Ethernet interface 0/1 and enable proxy arp on the interface.

Proxy arp is required since the remote IPsec client (in this case, the 9630) is on the same IP subnet as the SR4134's private interface. Proxy-arp allows the SR4134 to arp on behalf of the remote IPsec client.

```
SR/configure# interface ethernet 0/1
SR/configure/interface/ethernet (0/1)# ip address 47.17.124.43 255.255.255.0
SR/configure/interface/ethernet (0/1)# ip proxy_arp
```

5 Add the private IP address to the trusted zone

```
SR/configure/interface/ethernet (0/1)# crypto trusted
SR/configure/interface/ethernet (0/1)# exit
```

6 Show IP interfaces. Verify interface status is "up"

```
SR# show ip interfaces brief

Interface       Type                IP-Address/Mask  Status     Method
ethernet0/1     ETHERNET (802.3)    47.17.124.43/24  Up         MANUAL
ethernet0/2     ETHERNET (802.3)    10.1.1.1/24      Up         MANUAL
ethernet0/0     ETHERNET (802.3)    unassigned       Down       -
ethernet0/3     ETHERNET (802.3)    unassigned       Down       -
ethernet0/4     ETHERNET (802.3)    unassigned       Down       -
```

7 Add a static default route so the remote IP phone can communicate with the media server and other destinations within the corporate intranet. Display route table.

```
SR/configure# ip route 0.0.0.0/0 47.17.124.1

SR/configure# show ip route
Codes: C - connected, S - static,D - DHCP, R - RIP, B - BGP, M - MPLS
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default


IP Load balancing policy is per_flow

Gateway of last resort is 47.17.48.1 to network 0.0.0.0

S*     0.0.0.0/0 [1/0] via 47.17.124.1, ethernet0/1
C      10.1.1.0/24 is directly connected, ethernet0/2
C      47.17.48.0/24 is directly connected, ethernet0/1
C      127.0.0.0/8 is directly connected, lo0
```

8 Verify the SR4134 can ping the S8710 Media Server (135.20.146.10)

```
SR# ping 135.20.146.10

Pinging 135.20.146.10 (135.20.146.10); 64 bytes, timeout 5 seconds
!!!!!
Ping statistics for 135.20.146.10:
Packets: Transmitted 5, Received 5
Loss Rate 0%, approx. round-trip min/avg/max = 30/30/30 m
```

2.1.2 IPsec Configuration

In this section, IPsec will be configured on the SR4134 to allow the 9630 to establish an IPsec tunnel to it.

1 Configure an ike policy named "wan1", set the local interface to the SR4134s public IP address (10.1.1.1)

```
SR/configure# crypto
SR/configure/crypto# contivity-iras
SR/configure/crypto/contivity-iras# ike policy wan1
SR/configure/crypto/contivity-iras/ike/policy wan1# local-address 10.1.1.1
```

2 Configure the username and password to be used for remote IPsec client authentication. Here we will user "srtest" as the username and password

```
SR/configure/crypto/contivity-iras/ike/policy wan1# remote-id user-name "srtest"
password srtest
```

3 Configure an IKE proposal which uses diffe-hellman group 2 and triple DES encryption

```
SR/configure/crypto/contivity-iras/ike/policy wan1# proposal 1
SR/configure/crypto/contivity-iras/ike/policy wan1/proposal 1# dh-group group2
SR/configure/crypto/contivity-iras/ike/policy wan1/proposal 1# encryption-algorithm
3des-cbc
SR/configure/crypto/contivity-iras/ike/policy wan1/proposal 1# exit
```

4 Configure the remote IPsec client address pool. This address will be assigned to the 9630 phone after it has been authenticated by the SR4134. Enable NAT keepalive. Set the NAT keepalive interval to 20 seconds

```
SR/configure/crypto/contivity-iras/ike/policy wan1# client configuration
SR/configure/crypto/contivity-iras/ike/policy wan1/client/configuration# address-pool
1 47.17.124.72 47.17.124.74
SR/configure/crypto/contivity-iras/ike/policy wan1/client/configuration# keepalive
R2/configure/crypto/contivity-iras/ike/policy wan1/client/configuration/keepalive#
enable
SR/configure/crypto/contivity-iras/ike/policy wan1/client/configuration# nat-keepalive
20
```

5 Set the private side IP address to the trusted side IP address (47.17.124.43). Enable split tunnel mode and configure network routes which are reachable through the tunnel

```
SR/configure/crypto/contivity-iras/ike/policy wan1/client/configuration# private-side-
address 47.17.124.43
SR/configure/crypto/contivity-iras/ike/policy wan1/client/configuration# split-tunnel
SR/configure/crypto/contivity-iras/ike/policy wan1/client/configuration/split-tunnel#
mode enabled
SR/configure/crypto/contivity-iras/ike/policy wan1/client/configuration/split-tunnel#
network 47.17.0.0 16
```

```
SR/configure/crypto/contivity-iras/ike/policy wan1/client/configuration/split-tunnel#
network 135.0.0.0 8
```

6 Configure the banner text and exit out of ike configuration

```
SR/configure/crypto/contivity-iras/ike/policy wan1/client/configuration# banner-enable
SR/configure/crypto/contivity-iras/ike/policy wan1/client/configuration# banner-text
"Welcome"
SR/configure/crypto/contivity-iras/ike/policy wan1/client/configuration# exit 3
```

7 Configure an IPsec policy named "wan1" and specify the IPsec proposal. Set the SA lifetime to one hour. Exit to the top of the config hierarchy by

```
SR/configure/crypto/contivity-iras# ipsec policy wan1
SR/configure/crypto/contivity-iras/ipsec/policy wan1# proposal 1
SR/configure/crypto/contivity-iras/ipsec/policy wan1/proposal 1# lifetime seconds 3600
SR/configure/crypto/contivity-iras/ipsec/policy wan1/proposal 1# exit 5
```

The default IPsec proposal is triple DES with SHA-1. You must configure the same proposal on the 9630 IPsec client.

2.1.3 Firewall Configuration

In this section, the SR 4134 firewall will be configured so that an IPsec tunnel can be established to the SR4134 and secure voice and signaling traffic can be communicated between the 9630 IP phone and destinations located on the corporate intranet.

By default, the SR4134 contains two firewall zones, the internet zone and the corporate zone. The internet zone is the untrusted zone and, as its name implies, is the zone which interfaces with the untrusted side of the SR4134. Only one untrusted zone can be configured on the SR4134. The corp zone, on the other hand, is the trusted zone and interfaces with the trusted side of the SR4134. More than one trusted zone can be configured on the SR4134. However, for this technical configuration guide, the two default zones will be used: the internet zone and the corp zone.

1 Configure internet firewall rules to allow IPsec protocols: IKE, IKE-NAT, and ESP through the firewall.

By default, the internet firewall blocks all traffic originated from the untrusted side of the SR4134, therefore, before a tunnel can be established from the 9630 IP phone, we must configure some firewall policies to allow IPsec control traffic through the internet firewall.

```
SR/configure# firewall internet
SR/configure/firewall internet# policy 100 in service ike self
SR/configure/firewall internet# policy 101 in service ike-nat self
SR/configure/firewall internet# policy 102 in service contivity self
```

```
SR/configure/firewall internet# policy 103 in address 47.17.124.72 47.17.124.74
47.17.124.43 32 self
```

2 Show Internet firewall policies

```
SR/configure# show firewall policy internet
```

```
SR/configure# show firewall policy internet
Advanced: S - Self Traffic, F - Ftp-Filter, H - Http-Filter,
          R - Rpc-Filter, N - Nat-Ip/Nat-Pool, L - Logging,
          E - Policy Enabled, M - Smtp-Filter

Pri  Dir Source Addr        Destination Addr   Sport Dport Proto Action Advanced
---  --- -----------        ----------------   ----------------- ------ --------
100  in  any                any                -     ike   -     PERMIT SEL
101  in  any                any                -     ike-nat -     PERMIT SEL
102  in  any                any                -     contivity -     PERMIT SEL
103  in  47.17.124.72       47.17.124.43/32    any   any   any   PERMIT SEL
         47.17.124.74
1024 out any                any                any   any   any   PERMIT SEL
```

3 Configure the corp firewall to allow access to corporate resources, namely the media server and the destination IP phone. The policy will allow traffic sourced from the client range 47.17.124.72 to 47.17.124.74 and destined for networks 47.17.0.0/16 and 135.0.0.0/8.

```
SR/configure/firewall corp# policy 100 in address 47.17.124.72 47.17.124.74 47.17.0.0
16
SR/configure/firewall corp# policy 101 in address 47.17.124.72 47.17.124.74 135.0.0.0
8
```

4 Show firewall corp policies

```
SR/configure# show firewall policy corp
```

```
SR/configure# show firewall policy corp
Advanced: S - Self Traffic, F - Ftp-Filter, H - Http-Filter,
          R - Rpc-Filter, N - Nat-Ip/Nat-Pool, L - Logging,
          E - Policy Enabled, M - Smtp-Filter

Pri  Dir Source Addr        Destination Addr   Sport Dport Proto Action Advanced
---  --- -----------        ----------------   ----------------- ------ --------
100  in  47.17.124.72       47.17.0.0/16       any   any   any   PERMIT EL
         47.17.124.74
101  in  47.17.124.72       135.0.0.0/8        any   any   any   PERMIT EL
         47.17.124.74
1022 out any                any                any   any   any   PERMIT SEL
```

```
1023 in  any                any                 any    any    any    PERMIT SEL
1024 out any                any                 any    any    any    PERMIT EL
```

2.2 9630 IP Phone

This technical configuration guide assumes the reader is familiar with the operation and configuration of the Avaya 9630 IP phone and that the appropriate firmware is loaded and operational, including the IPsec client firmware. The 9630 phone must be running firmware version 3.1 or later to be interoperable with the SR4134/SR3130. The firmware version can be identified by viewing the version displayed as the phone is booting or by selecting the "Options & Settings" hard button when the phone is in operational mode.

2.2.1 IPsec Configuration

The following table shows the IPsec parameters that need to be configured in order to establish an IPsec tunnel to the SR4134. These IPsec parameters are configured while in "configuration" mode on the 9630 phone. You enter configuration mode in one of two ways:

1. During bootup, press "*" followed by access code 27238 #.
2. While the phone is operational, press Mute + 27238 + #.

Once in "configuration" mode, the IPsec parameters are configured under the "VPN" menu option

As an option, the 96xx IP phone can also be remotely configured by downloading the "46xxsettings.txt" during the boot process. The "46xxsettings.txt" is a text configuration file which you edit manually using a text editor. When the phone boots, instead of reading the local configuration file, it downloads the "46xxsettings.txt" file and configures itself based on the parameters in the file.

Whether using local or remote configuration, the VPN configuration is the same and you can use the VPN parameters shown in table 2 below as a guide when editing the "46xxsettings.txt" file.

2.2.1.1 IP Phone 9630 IPsec Parameters

Following is a list of the IPsec parameters used to establish an IPsec tunnel to the SR4134

Parameter	Value	Comment
VPN	Enabled	
VPN Vendor	Nortel	
Gateway Address	10.1.1.1	IP address of 4134 WAN Interface
External Phone IP Address	0.0.0.0	Obtained via DHCP
External Router	0.0.0.0	Obtained via DHCP
External Subnet Mask	0.0.0.0	Obtained via DHCP
Encapsulation	4500-4500	
Auth Type	Local Credentials	
VPN User Type	Any	

VPN User	srtest	User name for authentication
Password Type	Save in Flash	
User Password	srtest	Password for authentication
IKE ID Type	KEY_ID	
IKE Xchg Mode	Aggressive	
IKE DH Group	2	
IKE Auth Algorithm	SHA-1	
IKE Encryption Algorithm	3DES	
IKE Config Mode	Enabled	
IPsec PFS DH Group	NO PFS	
IPsec Encryption Algorithm	3DES	
IPsec Authentication Algorithm	SHA-1	
Protected n/w	0.0.0.0/0	

Table 2 – IP Phone 9630 IPsec Parameters

Once you exit out of “config mode” the 9630 will restart and attempt to establish the IPsec tunnel to the SR4134. You should see the words “Building VPN tunnel” displayed on the screen. Once the tunnel is up, the phone will conclude the boot-up process and register with the media server. You are now ready to make and receive secured voice calls.

2.3 Monitoring IPsec on SR4134

The SR4134 CLI provides a number of show commands which can be used to monitor the status of the IPsec tunnels.

1 Show IKE and IPsec Security Associations (SA)

```
R2# show crypto ike sa wan1
Policy                          Peer            State       Bytes       Transform
------                          ----            -----       -----       ---------
wan1                            10.1.1.2        SA_MATURE   1848        PRE-g2-3DES-SHA

R2# show crypto ipsec sa all
Policy                          Dest IP         SPI         Packets     Transform
------                          -------         ---         -------     ---------
INwan1                          10.1.1.1        b47be719    11419       ESP-3DES-SHA-TU
```

```
wan1                            10.1.1.2          8cb8d25e      11450        ESP-3DES-SHA-TU
```

2 Show remote IPsec client information

```
R2# show crypto clients contivity

Client Address  Client Id        Policy               Type
--------------  ---------        ------               ----
10.1.1.2        srtest           wan1:47.17.124.72    Contivity
```

3 Show internet and corp firewall connections

```
R2# show firewall connections internet

P: Protocol. T - TCP, U - UDP, I - ICMP, A - AH, E - ESP, G - GRE, H - HTTP(S), O - Other
Life: Specified in Seconds

map name is   internet
Max Connections  7500
Active Connections  3

P Source                Dest                Life   Bytes
- ------                ----                ----   -----
U 10.1.1.2:10009        10.1.1.1:4500       60     11303
  10.1.1.1:4500         10.1.1.2:10009      60     0
U 10.1.1.2:10000        10.1.1.1:500        33     304
  10.1.1.1:500          10.1.1.2:10000      33     224
T 47.17.124.72:26378    135.20.146.10:1720  600    26670
  135.20.146.10:1720    47.17.124.72:26378  600    372643

R2# show firewall connections corp

P: Protocol. T - TCP, U - UDP, I - ICMP, A - AH, E - ESP, G - GRE, H - HTTP(S), O - Other
Life: Specified in Seconds

map name is   corp
Max Connections  2500
Active Connections  1

P Source                Dest                Life   Bytes
- ------                ----                ----   -----
T 47.17.124.249:1471    47.17.124.43:23     600    106
  47.17.124.43:23       47.17.124.249:1471  600    3720
```

© 2011 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. and are registered in the United States and other countries. All trademarks identified by ®, TM or SM are registered marks, trademarks, and service marks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. Avaya may also have trademark rights in other terms used herein. References to Avaya include the Nortel Enterprise business, which was acquired as of December 18, 2009.