Avaya Secure Router 2330 / 4134

Advanced gateway 2330

Avaya 9600 Series IP Phones

**Engineering**

# > Secure Router IPsec Interoperability with Avaya 9600 IP Phones Technical Configuration Guide

**Avaya Data Solutions**

**Document Date: March 2011**

**Document Number: NN48500-620**

**Document Version: 1.0**

**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 the Avaya Secure Router to interoperate with the IPsec client on Avaya's 9600 Series IP Phones. This enables the Avaya 9600 IP Phones to terminate a secure connection to the Secure Router via IPsec Virtual Private Network (VPN) technology.

# Revision Control

| No | Date | Version | Revised By | Remarks |
|---|---|---|---|---|
| 1 | March 2011 | 1.0 | D. Passamonte | Initial Draft |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Table of Contents

Figures ..... 5
Tables ..... 6
1. Introduction ..... 8
1.1 Hardware ..... 8
1.2 Network Topology ..... 9
1.3 Test Performed ..... 10
2. Configuration ..... 11
2.1 Avaya 9600 Series IP Phone ..... 11
2.2 Secure Router 4134 ..... 12
3. Appendix ..... 15
3.1 Secure Router 4134 Configuration ..... 15
4. Reference Documentation ..... 31

# Figures

Figure 2.2 – Network Topology ..... 9

# Tables

Table 1.0 – Applicable Secure Router Platforms ..... 8
Table 1.3 – Test Performed ..... 10

# 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 describes the steps required to configure the Avaya Secure Router in a way that will interoperate with the Avaya 9600 IPsec client. This solution provides customers with the ability to deploy Avaya 9600 IP Phones securely, using IPsec Virtual Private Network 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 | v10.3 | Up to 1000 Tunnels |
| Secure Router 2330 with VPN Encryption Module (SCIM) | v10.3 | Up to 100 Tunnels |
| Advanced Gateway with Secure Router Upgrade License and VPN Encryption Module (SCIM) | v10.3 | Up to 100 Tunnels |

**Table 1.0 – Applicable Secure Router Platforms**

## 1.1 Hardware

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

- Secure Router 4134 version 10.3
- Avaya 9600 version 6.0
- Avaya S8730 Media Server version 5.2.1
- Avaya G650 Media Gateway version 6.0

## 1.2 Network Topology

The following network topology was used to validate the configuration outlined in this technical configuration guide:

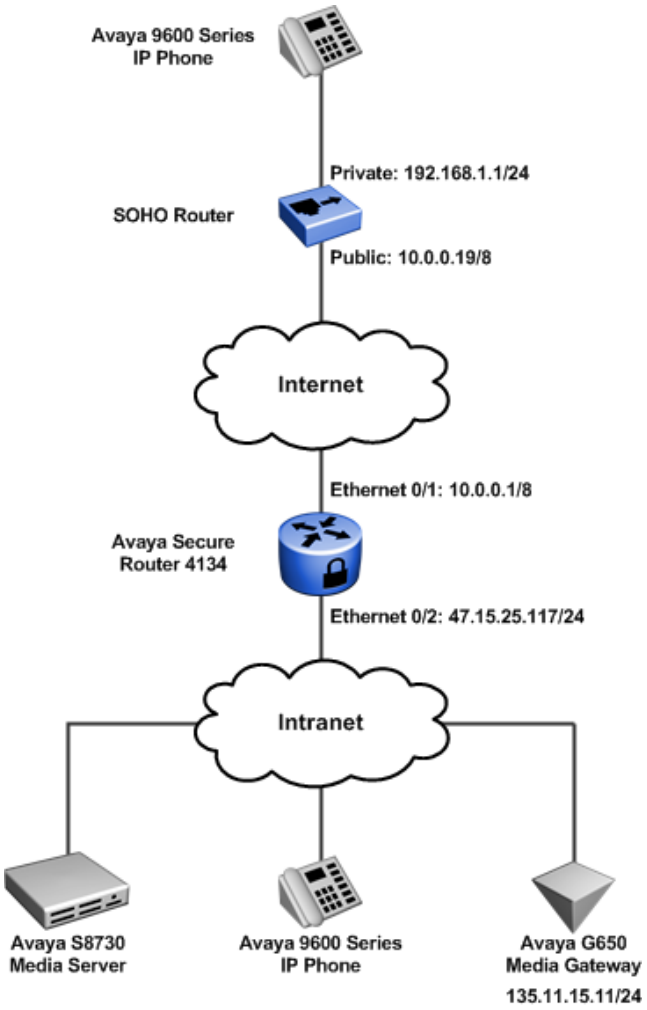


**Figure 2.2 – Network Topology**

## 1.3 Test Performed

This test was performed using the native IPsec client of the 9600 IP phone. The Secure Router 4134 was configured for a “contivity-iras” to provide an interoperable solution. The following functionality was tested:

| Test Case | Description | Result |
|---|---|---|
| Successful IPsec connection using PSK | This test case demonstrated the ability of the remote 9600 to create an IPsec connection to the Secure Router using pre-shared keys, ESP and receive IP address during MODE-CONFIG. | Passed |
| Remote 9600 ability to make a phone call | This test case demonstrated the ability of the remote 9600 to successfully make a phone call to the 9600 on the Intranet. | Passed |
| Remote 9600 ability to receive a phone call | This test case demonstrated the ability of the remote 9600 to successfully receive a phone call to the 9600 on the Intranet. | Passed |
| Verify two way speech path | This test case demonstrated the ability for a two way conversation between the remote and local phones. Voice traffic was successfully sent and received by both phones as well as evidenced by conversations between two individuals over the phones used in this test. | Passed |
| Successful rekey on hook | This test case demonstrated the ability of the remote 9600 and the Secure Router 4134 to successfully rekey phase 2 of the IPsec Security Association while the 9600 phones were ‘on hook’. | Passed |
| Phone maintained registration to the call server with no on hook for 24 hours | This test case demonstrated the ability of the remote 9600 to successfully maintain an IPsec connection while ‘on-hook’ for a prolonged period. The 9600 phone maintained registration to the call server throughout the period of the test. | Passed |

**Table 1.3 – Test Performed**

# 2. Configuration

## 2.1 Avaya 9600 Series IP Phone

The following highlights the network settings defined on the Avaya 9600 Series IP Phone to establish a secure IPsec VPN tunnel to the Secure Router 4134:

| Prompt | Value |
|---|---|
| VPN | Enabled |
| VPN Vendor | Nortel |
| Gateway Address | 10.0.0.1 |
| External Phone IP Address | 0.0.0.0 |
| External Router | 192.168.1.1 |
| External Subnet Mask | 255.255.255.0 |
| Encapsulation | Disabled |
| Auth Type | Local Credentials |
| VPN User Type | Any |
| VPN User | voip |
| Password Type | Save in Flash |
| User Password | voip |
| IKE ID Type | KEY_ID |
| IKE Xchg Mode | Aggressive |
| IKE DH Group | 2 |
| IKS Auth Algorithm | 3DES |
| IKE Encryption Algorithm | SHA-1 |
| 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 |

| | |
|---|---|
| IKE over TCP | Never |

## 2.2 Secure Router 4134

The following highlights the Interface, IPsec and Firewall configuration defined on the Secure Router 4134 to support IPsec VPN tunnels from Avaya 9600 Series IP Phones:

Note – Interface, IPsec and firewall configurations are commented for additional clarity. The startup configuration used for this test is provided in the appendix.

**1 Interface Configuration:**

```
interface ethernet 0/1
  ip address 10.0.0.1 255.0.0.0
    ip rip send version 2
    ip rip receive version 2
  aaa
    exit aaa
## Public Interface
crypto untrusted
  qos
    chassis
      exit chassis
    exit qos
  exit ethernet
interface ethernet 0/2
  ip address 47.17.25.117 255.255.255.0
## proxy arp required so SR arps on behalf of IPsec RAS clients
  ip proxy_arp
  aaa
    exit aaa
## Private Interface
  crypto trusted
  qos
    chassis
      exit chassis
    exit qos
  exit Ethernet
```

## 2 IPsec Configuration:

```
crypto
  dynamic
    exit dynamic
## contivity-iras used for interoperability with 9600
  contivity-iras
    ike policy cont1
## local-address is the public interface (WAN) of the Secure Router
        local-address 10.0.0.1
## remote-id username test strings must be quoted, followed by password
        remote-id user-name "voip" voip
        proposal 1
          dh-group group2
          encryption-algorithm 3des-cbc
          exit proposal
        client configuration
            address-pool 1 47.17.25.120 47.17.25.125
## private-side address is the LAN interface of the router. Crypto TRUSTED.
            private-side-address 47.17.25.117
            keepalive
              exit keepalive
            split-tunnel
              mode enabled
              network 47.17.25.0 24
              exit split-tunnel
            nat-keepalive 40
            exit configuration
        exit policy
    ipsec policy cont1
        proposal 1
          lifetime seconds 3600
          exit proposal
        exit policy
    exit contivity-iras
  no keepalive mode periodic
  pmtu
    exit pmtu
```

```
  qos
    chassis
      exit chassis
    exit qos
  exit crypto
```

## 3 Firewall Configuration:

```
firewall internet
  interface ethernet0/1
  policy 100 in permit service ike self
    exit policy
  policy 101 in permit protocol udp port 4500 4500  self
    exit policy
## Allow encapsulated packets for ipsec policy processing.
  policy 102 in permit address 47.17.25.120 47.17.25.125 47.17.25.117 32  self
    exit policy
## Permit USDP for ESP traffic (IPsec)
  policy 103 in permit protocol tcp port any 17  self
    exit policy
## Added for ping testing during setup, an be left out, but SR will not reply to ping.
  policy 104 in permit protocol icmp self
    exit policy
  exit firewall
firewall corp
  interface ethernet0/2 ethernet6/2
  policy 10 in permit
    exit policy
## Allow encapsulated packets for ipsec policy processing.
  policy 100 in permit address 47.17.25.120 47.17.25.125 47.17.25.0 24
    exit policy
  policy 1024 out permit
    exit policy
  exit firewall
```

# 3. Appendix

## 3.1 Secure Router 4134 Configuration

The following provides the startup configuration from the Secure Router 4134 used in this technical configuration guide:

**Secure Router 4134 Startup Configuration:**

```
system logging
  console
    priority crit
    exit console
  syslog
    module alarms local0 none
    module dos local0 none
    module forwarding local0 none
    module voip-ssm-cdr local0 none
    module voip-cdr local0 none
    exit syslog
  exit logging
hostname plm_4134-1
log utc
event
  exit event
usb
  exit usb
terminal
  exit terminal
qos
  module
    exit module
  chassis
    exit chassis
  exit qos
module t1 1/1
  alarms
    thresholds
      exit thresholds
    exit alarms
  linemode
    exit linemode
  exit t1
module t1 1/2
```

```
  alarms
    thresholds
      exit thresholds
    exit alarms
  linemode
    exit linemode
  exit t1
module hssi 5/1
  clock_source internal
  clock_rate 52000000
  crc 16
  mode dce
  data_mode normal
  exit hssi
aaa
  tacacs
    exit tacacs
  radius
    primary_server
      exit primary_server
    secondary_server
      exit secondary_server
    exit radius
  exit aaa
vlan database
  exit database
vlan classification
  exit classification
bridge
 mstp
   exit mstp
  exit bridge
lacp
  exit lacp
interface loopback routerid
  ip address 100.0.0.100 255.0.0.0
  exit loopback
interface ethernet 0/1
  ip address 10.0.0.1 255.0.0.0
    ip rip send version 2
    ip rip receive version 2
  aaa
    exit aaa
  crypto untrusted
```

```
  qos
    chassis
      exit chassis
    exit qos
  exit ethernet
interface ethernet 0/2
  ip address 47.17.25.117 255.255.255.0
  ip proxy_arp
  aaa
    exit aaa
  crypto trusted
  qos
    chassis
      exit chassis
    exit qos
  exit ethernet
interface ethernet 0/3
  aaa
    exit aaa
  qos
    chassis
      exit chassis
    exit qos
  exit ethernet
interface ethernet 6/1
  ip address 30.1.3.1 255.255.255.0
  aaa
    exit aaa
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/2
  ip address 31.1.2.1 255.255.255.0
  aaa
    exit aaa
  crypto trusted
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/3
```

```
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/4
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/5
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/6
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/7
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
```

```
interface ethernet 6/8
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/9
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/10
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/11
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/12
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
```

```
  exit ethernet
interface ethernet 6/13
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/14
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/15
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/16
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/17
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
```

```
    exit qos
  exit ethernet
interface ethernet 6/18
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/19
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/20
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/21
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/22
  aaa
    exit aaa
  switchport
  qos
    module
```

```
      exit module
    exit qos
  exit ethernet
interface ethernet 6/23
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 6/24
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 7/1
  aaa
    exit aaa
  switchport
  qos
    module
      ingress-buffer-limit 170
      egress-buffer-limit 176
      xon-limit 150
      xoff-limit 167
      queue 1
        queue-limit 16
        exit queue
      queue 2
        queue-limit 16
        exit queue
      queue 3
        queue-limit 16
        exit queue
      queue 4
        queue-limit 16
        exit queue
      queue 5
```

```
        queue-limit 32
        exit queue
      queue 6
        queue-limit 32
        exit queue
      queue 7
        queue-limit 32
        exit queue
      queue 8
        queue-limit 32
        exit queue
      exit module
    exit qos
  exit ethernet
interface ethernet 7/2
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 7/3
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 7/4
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 7/5
  aaa
    exit aaa
```

```
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 7/6
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 7/7
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 7/8
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 7/9
  aaa
    exit aaa
  switchport
  qos
    module
      exit module
    exit qos
  exit ethernet
interface ethernet 7/10
  aaa
```

```
    exit aaa
  switchport
  qos
    module
      ingress-buffer-limit 170
      egress-buffer-limit 176
      xon-limit 150
      xoff-limit 167
      queue 1
        queue-limit 16
        exit queue
      queue 2
        queue-limit 16
        exit queue
      queue 3
        queue-limit 16
        exit queue
      queue 4
        queue-limit 16
        exit queue
      queue 5
        queue-limit 32
        exit queue
      queue 6
        queue-limit 32
        exit queue
      queue 7
        queue-limit 32
        exit queue
      queue 8
        queue-limit 32
        exit queue
      exit module
    exit qos
  exit ethernet
interface bundle hssi_wan
  link hssi 5/1
  encapsulation ppp
  ip address 40.0.0.1 255.255.255.0
    ip rip send version 2
    ip rip receive version 2
  ppp pap
    exit pap
  ppp chap
```

```
    exit chap
  ppp authentication-database local
  aaa
    exit aaa
  qos
    chassis
      exit chassis
    exit qos
  exit bundle
interface bundle t1_wan2
  ppp pap
    exit pap
  ppp chap
    exit chap
  aaa
    exit aaa
  qos
    chassis
      exit chassis
    exit qos
  exit bundle
interface bundle t1_wan
  link t1 1/1
  encapsulation ppp
  ip address 60.0.0.1 255.0.0.0
    ip rip send version 2
    ip rip receive version 2
  ppp pap
    exit pap
  ppp chap
    exit chap
  ppp authentication-database local
  aaa
    exit aaa
  qos
    chassis
      exit chassis
    exit qos
  exit bundle
interface console
  aaa
    exit aaa
  exit console
gvrp
```

```
  exit gvrp
snmp-server
  chassis-id plm_4134-1
  enable traps
    exit traps
  exit snmp-server
rmon
  exit rmon
poe portmode 6/1 1
poe portpower 6/1
oam
  cfm
    enable
    ethtype 88e6
    exit cfm
  exit oam
ftp_server
icmp_timestamp
telnet_server
telnet_banner
  exit telnet_banner
sntp
  exit sntp
reverse_telnet
  set_baud_rate 56000
  exit reverse_telnet
router-id 100.0.0.100
ip proxy-dns
  exit proxy-dns
ip load-balancing per-flow
ip icmp rate-limit 500
ip dhcps
  interface ethernet0/1
  relay 11.1.1.254 11.1.1.0
  enable
  exit dhcps
ip route 0.0.0.0/0 47.17.25.1
ip route 14.0.0.0/8 hssi_wan
ipv6 icmp rate-limit 500
ipv6 unicast-routing
ipv6 load-balancing per-flow
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.255.255.255 area 0.0.0.0
```

```
 network 40.0.0.0 0.255.255.255 area 0.0.0.0
  exit ospf
router rip
 network t1_wan
 network ethernet0/1
 neighbor 60.0.0.2
  exit rip
mpls tunnel-mode uniform
firewall global
  algs
    dns
      exit dns
    exit algs
  max-connection-limit self 2048
  bypass-trusted
  exit firewall
firewall internet
  interface ethernet0/1
  policy 100 in permit service ike self
    exit policy
  policy 101 in permit protocol udp port 4500 4500  self
    exit policy
  policy 102 in permit address 47.17.25.120 47.17.25.125 47.17.25.117 32  self
    exit policy
  policy 103 in permit protocol tcp port any 17  self
    exit policy
  policy 104 in permit protocol icmp self
    exit policy
  exit firewall
firewall corp
  interface ethernet0/2 ethernet6/2
  policy 10 in permit
    exit policy
  policy 100 in permit address 47.17.25.120 47.17.25.125 47.17.25.0 24
    exit policy
  policy 1024 out permit
    exit policy
  exit firewall
crypto
  dynamic
    exit dynamic
  contivity-iras
    ike policy cont1
        local-address 10.0.0.1
```

```
        remote-id user-name "voip" voip
        proposal 1
          dh-group group2
          encryption-algorithm 3des-cbc
          exit proposal
        client configuration
            address-pool 1 47.17.25.120 47.17.25.125
            private-side-address 47.17.25.117
            keepalive
              exit keepalive
            split-tunnel
              mode enabled
              network 47.17.25.0 24
              exit split-tunnel
            nat-keepalive 40
            exit configuration
        exit policy
    ipsec policy cont1
        proposal 1
          lifetime seconds 3600
          exit proposal
        exit policy
    exit contivity-iras
  no keepalive mode periodic
  pmtu
    exit pmtu
  qos
    chassis
      exit chassis
    exit qos
  exit crypto
voice class
  exit class
voice service voip
  sip
    exit sip
  fax rate-management transferredTCF
  codec 1 g711ulaw 160
  ssm
    registrar
      exit registrar
    dialplan
      exit dialplan
    digest-auth
```

```
      exit digest-auth
    sip-server
      exit sip-server
    cac
      exit cac
    sessiontimer
      exit sessiontimer
    protocol-header
      exit protocol-header
    provisioning
      exit provisioning
    exit ssm
  exit voip
voice call
  exit call
voice dsp
  exit dsp
sip-ua
  keepalive timer 60
  exit sip-ua
dst
  no enable
  exit dst
```

# 4. Reference Documentation

| Publication Number | Description |
|---|---|
| 16-602968 | VPN Setup Guide for 9600 Series IP Telephones Release 3.1 |
| NN47263 | Security Configuration and Management – Avaya Secure Router 2330/4134 |
| | |
| | |
| | |
| | |
| | |