Secure Router 4134/2330

Software Release 10.3.5 Release Notes

1. Release Summary

Release Date:	January 2, 2014
Purpose:	Software release to consolidate multiple customer patch releases along with support for AG2330. New features and enhancements done in this release are explained in this document.

2. Notes for Upgrade

Please refer to the configuration guide, "Commissioning the Avaya Secure Router 4134 and 2330", release version 10.3, available at http://www.avaya.com/support for details on how to upgrade your Secure Router unit.

File Names for This Release

Description	File Size	Image Version	Boot Rom Version	File Name
Secure Router 4134 Application Image	29,597,192 bytes	10.3.5	62	SR4134.Z
Secure Router 2330 Application Image	30,647,461 bytes	10.3.5	52	SR2330.Z
Advanced Gateway 2330 Application Image	30,647,461 bytes	10.3.5	52	AG2330.Z

3. Version of Previous Release

Software Version 10.3.4.15

4. Compatibility

Phone compatibility: Avaya H.323 Phones VPN client is compatible with the Secure Router contivity-iras remote access server. The following H.323 phone firmware versions are compatible:
96x0 phones - firmware version 3.1.03 or later.
96x1 phones - firmware version 6.3.0.37 or later.
11xx phones - firmware version 062xC8Q or later.

Avaya SIP Phones utilize SSL encryption as part of the SIP protocol and do not require a separate VPN client.
Note: The 11xx phone firmware does not generate the proper IKE communication parameters if the VPN client username entered contains capital letters. Use only lower case letters for the VPN client username on an 11xx phone.

5. New Features in R10.3.5

5.1. IPFix:

IPFIX defines a common, universal standard of export for IP flow information used by network management, and allows to facilitate services such as monitoring, measurement, accounting, and billing. There are 2 key components in enabling IPFIX:

1. Defining the interfaces where sampling should be enabled
2. Defining the collector where flow information will be exported

Here is a sample configuration:

Step 1: Enabling IPFIX and configuration of Flow Collector.

```
ip flow-export enable
ip flow-export collector wins8 47.152.227.80 6343
```

Step 2: Enabling monitoring on desired interface with defining the sampling value.

```
interface ethernet 6/7
  ip flow-export flow-capture ingress standard
  ip flow-export flow-sampling 5000
  exit ethernet
interface ethernet 6/8
  ip flow-export flow-capture ingress standard
  ip flow-export flow-sampling 5000
```

5.2. Interoperability with Silverpeak NX WAN optimization:

Secure Router now supports interoperability with Silverpeak NX. The Silverpeak product is not running on the Secure Router in this case. The configuration guide NN48500-623: Avaya Secure Router 4134 with Silverpeak NX Wan optimization provides more details.

5.3. GRIP 9765/Dual Registration:

SR/AG can be deployed as a branch Gateway with dual Session Manager at the headquarters. If the primary SIP server goes down, AG/SR fails over to the Secondary SIP server. FXS lines registered earlier with Primary SIP-Server now registers with the Secondary SIP-Server. When the Primary SIP server comes back up, AG/SR falls back to the Primary SIP server and the FXS lines register back with the Primary SIP server. If SSM is configured as tertiary sip server and if both the primary and secondary SM goes down, AG/SR fails over to the tertiary server (SSM).

The following CLI output shows an example:

```
AG2330# show sip-ua status
SIP User Agent Status
SIP User Agent for UDP : DISABLED
SIP User Agent for TCP : ENABLED
SIP User Agent bind status(signaling): ENABLED
SIP max-forwards : 70
Primary   SIP server : ipv4:10.133.133.83:5060
```

```
Secondary SIP server : ipv4:192.168.129.7:5060
Tertiary  SIP server : ipv4:192.168.129.90:5060
Registrar server : ipv4:10.133.133.83:5060 expires 3600
Outbound Proxy :  n/a
Authentication username : n/a
Authentication password : n/a
Keepalive Timer : 60
Keepalive Trigger Count : 1
Keepalive Retry Count : 1
Keepalive Target Primary SIP Server and Registrar : (UP & ACTIVE)
Keepalive Target Secondary SIP Server and Registrar : (UP)
Keepalive Target Tertiary SIP Server  : (UP)
SIP Domain :    dns:sr.avaya.com
Register Server: None
SDP application configuration:
Version line (v=) required
Session name line (s=) required
Timespec line (t=) required
Network types supported: IN
Address types supported: ipv4
Transport types supported: RTP/AVP TCP

AG2330# show sip-ua register status
Line      peer                expires(sec)  registered    registrar
37        5151234567          3600          yes           sr.avaya.com(P)
38        5151234590          3600          yes           sr.avaya.com(P)
```

5.4. CPU Monitoring:

Secure Router's design utilizes both a SW and HW forwarding engine in combination. SW forwarding is meant as a cost effective strategy in providing data forwarding over low bandwidth TDM WAN links, as well as Ethernet connectivity that does not require high throughput.

With using the SW forwarding design, it is desirable to provide means where the utilization can be measured and gauged. This data will provide details on the load of the system and can be used to estimate the ability of the system to handle bursts of traffic under the current condition.

For this release, we will provide an Enterprise MIB where the utilization will be represented as a scalar with 3 possible values:

1. GREEN: System is under normal load and reasonable traffic burst can be handled.
2. YELLOW: System is fully utilized where short data burst may still be handled.
3. RED: System is under heavy load, and further data burst will cause data drops.

The CPU Monitoring feature provides a means for early detection of over stress condition of the system CPU, which could lead to forwarding loss over the chassis interfaces on SR4134, or IP Forwarding on the SR2330 platform.

With this feature, a new Enterprise MIB and an SNMP Trap are defined that allow live monitoring of Secure Router. The MIB tree is defined in the context of 1.3.6.1.4.1.562.73.1.1.1.25 (PROCESS-MIB).

The SNMP trap allows for notification when the CPU state changes, for example, from "GREEN" to "YELLOW". The trap is defined as "cpuTotalThresholdTrap"

The SNMP Enterprise MIB allows for polling of the CPU state from the Management station.

5.4.1. Feature Configuration:

The feature is started by command executed from CLI. This feature can be started by default when the system starts next time by saving the configuration (Ex: using "save local" command).

```
SR4134/configure# process cpu
SR4134/configure/process cpu# start-process
```

Command to display the CPU utilization:

```
SR4134# show processes cpu utilization
CPU %Utilization: 10Sec - 51, 1Min(Peak/Avg) - 52/51, 5Min(Peak/Avg) -
54/51
```

This particular output means that:

a) The CPU utilization in the last 10 seconds is 51%.
b) The peak and average CPU utilization during the last 1 minute is 52% and 51% respectively.
c) The peak and average CPU utilization during the last 5 minutes is 54% and 51% respectively.

This show command also has multiple options to display more information on the CPU utilization.

SNMP trap can be enabled to send notification when the CPU state changes, for example, from “GREEN” to “YELLOW”. This SNMP trap can be enabled using the command:

```
SR/configure/snmp-server/enable/traps# cpu total
```

The CPU state can also be shown from the CLI context by using this command:

```
SR4134# show processes cpu color
Color : Red
```

5.5. IPSLA Enhancements:

The Secure Router now supports IPSLA monitoring capability with the ability to expand the number of IPSLA items being tracked and for the router to be able to take action based on IPSLA thresholds being reached.

The number of IPSLA items being tracked has been increased to 25.

5.5.1. IPSLA – Static Routing Integration

The drive for this feature stems from the ease in deploying static routing with tunnels as a basis for network redundancy. With static routes configured in directly connected peering, in most cases the downing of the peer device would result in the operational downing of the connected interface too. This would in turn cause the withdrawing of the associated static route from the forwarding table. However, in cases where the peer is connected through a switch or over a virtual tunnel, peer down event may not trigger the withdrawal of the static route as the physical connectivity is still available. This would result in black holing of the data traffic streams destined over these static routes as switchover to alternate routes will not happen.

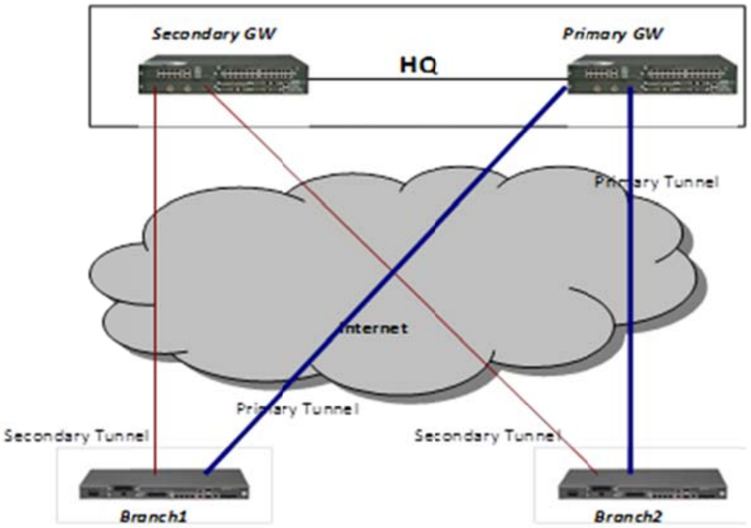

Figure 1: Static Route Deployment Scenario

The above deployment diagram illustrates a sample deployment with 2 Branch offices connected to HQ through tunnels. It's a hub and spoke topology where each branch can communicate to each other through the HQ. HQ (hub) has two routers (primary and backup) for redundancy. Each branch has a primary set of static routes using primary tunnel and high distance (secondary) set of static routes using secondary tunnel.

If Primary GW goes down, the tunnel might still stay up and thus black-hole all communication. If an IPSLA tracker is created on a branch router for the primary GW and is associated with static routes, then once the primary GW goes down, the tracker will fail and will cause static route also to go down. Once the primary set of static routes go down because of the tracker failure, the secondary set of static routes will take over, resuming communication using the secondary GW.

5.5.1.1. Feature Configurations

Step 1: Define the standard SLA profile and Tracking ID – in this example, we are defining an icmp-echo test to destination 11.1.1.1 with the condition of no packet loss in 2 out of 4 tests.

```
sla profile 2
  icmp-echo 11.1.1.1
  action packet-loss
  threshold-type xofy
  threshold-value 2 4
  exit profile
sla schedule 2
track 20
  service-sla-profile 2
  exit track
```

Step 2: Associate the SLA tracker with a static route:

```
ip route 192.168.225.1 255.255.255.0 track 20
```

5.5.1.2. Feature Usage and Caveats

1. Based on the configured SLA parameter - threshold violation will trigger the permanent withdrawing of the associated Static Route entry from the forwarding table. This is to avoid intermittent network outage resulting in the continuous addition/withdrawal of static routes.

2. Withdrawing of specific static route will have normal impact on data forwarding – that is, using

Longest Prefix Match algorithm the next best route will be inserted into the forwarding table.

3. Administrator action is required to reset the state of the static route:

   ```
   clear ip route track <trackerTag>
   ```

   In the case where this static route is withdrawn due to IPSLA failure, the specified route will be re-inserted into the routing table. In addition, the IPSLA test associated with this route will be restarted.

4. To help identify Static Route that is withdrawn due to IPSLA event, a new identifier "!" is added to the show ip route database:

   ```
   ! - IPSLA disabled route
   ```

   Any route mark with this flag indicates that it is not selected due to IPSLA test failures.

5. Since a tracker can be associated with multiple clients, any client that resets the tracker will also impact all existing listeners. For example, in the case where a tracker is associated with 2 static routes – any one of the static route client can reset the tracker (resetting IPSLA test). All associated clients will then receive the common event once the new test set completes. However, note that this doesn't clear the state of the client and this must be done individually.

5.5.2. IPSLA – OSPF Integration

Now user has the capability of influencing the OSPF behavior on an interface when IPSLA threshold violation is defected. Specifically, a new option is added to each IPSLA tracker object that cease OSPF on the configured interface. The IPSLA objects will be associated with OSPF at interface level under the "ip ospf" context.

5.5.2.1. Feature Configurations

Step 1: Define the standard SLA profile and Tracking ID – in this example, we are defining an icmp-echo test to destination 11.1.1.1 with the condition of no packet loss in 2 out of 4 tests.

```
      sla profile 2
        icmp-echo 11.1.1.1
        action packet-loss
        threshold-type xofy
        threshold-value 2 4
        exit profile
      sla schedule 2
      track 20
        service-sla-profile 2
        exit track
```

Step 2: Associate the SLA tracker with OSPF at the interface level:

```
      interface Ethernet 0/1
        ip ospf sla-tracker 20 disable
        exit
```

5.5.2.2. Feature Usage and Caveats

1. Based on the configured SLA parameter - threshold violation will trigger the permanent down of the configured OSPF adjacency. Consider the following:

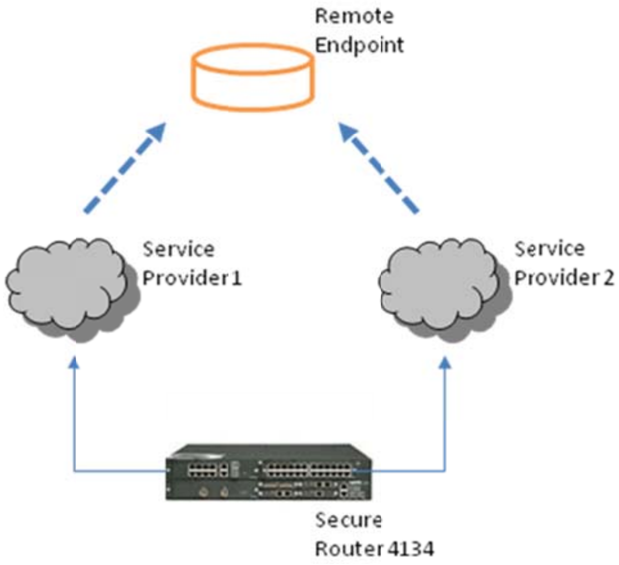

Figure 2: Dual Home OSPF Topology

Using this topology, Service Provider 1 (SP1) provides primary connectivity to the remote end point; while Service Provider 2 (SP2) is the backup link – traffic forwarding is controlled using routing cost adjustments and not ECMP (thus only one Service Provider carries traffic at any point in time). IPSLA is configured to monitor the link performance when connected to the Remote Endpoint.

Consider the scenario where the connectivity performance through SP1 decreases, thus triggering the threshold violation. With IPSLA enhancement, the adjacency with SP1 will be brought down resulting in all traffic being redirected to SP2. However, with this change, IPSLA monitoring will be re-established going through SP2 – if we automatically restore on the adjacency with SP1. This will result in a continuous flip-flop of the network traffic.

2. OSPF adjacency down will have normal impact on data forwarding – that is, using Longest Prefix Match algorithm the next best route will be inserted into the forwarding table.

3. Administrator action is required to reset the state of OSPF. 2 commands are available :

   ```
   a) clear ip ospf sla-tracker 20 disable
   ```

   This clears this specific instance of OSPF association and the associated IPSLA tracker.

   ```
   b) clear ip ospf process
   ```

   This clears all instances of OSPF on the router along with all the associated IPSLA trackers.

4. To help identify OSPF Route that is withdrawn due to IPSLA event, a new identifier “!” is added to the show ip route database:

   ```
   ! - IPSLA disabled route
   ```

   Any route mark with this flag indicates it is not selected due to IPSLA test failures.

5. Since a tracker can be associated with multiple clients, any client that resets the tracker will also impact all existing listener. For example, in the case where a tracker is associated with 2 OSPF adjacencies – any one of the client can reset the tracker (resetting IPSLA test). All associated client will then receive the common event once the new test set completes. However, note that this does not clear the state of the client as this must be done individually.

5.6. GRIP 9102 - Multicast Forwarding of traffic originating from a non-local source:

This enhancement is specific to those customers with a need to forward multicast traffic received from a source whose IP address is not in the same subnet as the IP address configured on the interface connected to that network segment.

The configuration to be done on Secure Router for this type of traffic forwarding is only to add a static route on the router with the interface connected to the source subnet as the outgoing interface:

```
SR4134-1/configure# ip route 1.1.1.0/24 ethernet6/2
```

The following example shows multicast traffic with source ip 1.1.1.100 coming in through the interface ethernet6/2 (which is configured with 100.1.1.1/24 address). A multicast record is created as follows and traffic is forwarded out through vlan101 interface:

```
SR4134-1/configure# show ip mroute
IP Multicast Forwarding Table
(Source ,Group), Uptime/Expiry
Incoming Interface: Interface Name, Owner
Outgoing Interface List: Interface Name, Uptime (TTL Threshold)
1 forwarding entries (0 temporary, 0 negative)
(1.1.1.100, 224.1.1.1), 00:03:01/00:02:00
Incoming interface: ethernet6/2, PIM-SM,
Outgoing interface list:
      vlan101  ,  00:03:01
```

5.7. Enhancement for displaying running and start-up configuration:

This feature introduces the following options to commands “show running-config” & “show startup-config”, so that only specific parts of the configuration can be displayed:

begin: displays the commands configured starting with the string provided.

include: displays the commands configured whose parts match the string provided.

exclude: displays all the commands configured except those that match the string provided.

include-section: displays all the commands configured which match the string provided. In addition, the commands which are part of the tree of these matching commands are also displayed.

exclude-section: displays all the commands configured except those matching the string. In addition, commands which are part of the tree of these matching commands are not displayed.

The optional <string> is formed by 3 substrings ie. <string1> <string2> <string3>. Each of the substrings i.e, string1, string2, string3 will consist a maximum of 40-characters each.

5.7.1.Usage:

running-config

```
SR# show running-config ?
 begin           Displays lines starting with the string
 include         Displays lines containing the string
 exclude         Displays lines not containing the string
 include-section Displays lines containing and associated with the
                 string
 exclude-section Displays lines not containing and not associated with
                 the string
      <cr>
```

startup-config

```
SR# show startup-config ?
  file             local file name. (default: system.cfg)
  begin            Displays lines starting with the string
  include          Displays lines containing the string
  exclude          Displays lines not containing the string
  include-section  Displays lines containing and associated with the
                   string
  exclude-section  Displays lines not containing and not associated
                   with the string
      <cr>
```

5.7.2. CLI examples:

Consider the following output for the examples.

```
SR# show running-config
Retrieving configuration... please wait

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
    module voip-gwy local0 none
    exit syslog
  exit logging
hostname SR
log utc
event
  exit event
terminal
  exit terminal
qos
  module
    exit module
  chassis
    exit chassis
  exit qos
module serial 1/1
  exit serial
module serial 1/2
  exit serial
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 ethernet 0/1
  ip address 192.168.90.2 255.255.192.0
  aaa
    exit aaa
  qos
    module
      exit module
    chassis
      exit chassis
    exit qos
  exit ethernet
interface ethernet 0/2
  ip address 10.1.1.1 255.255.255.0
  aaa
    exit aaa
  qos
    module
      exit module
    chassis
      exit chassis
    exit qos
  exit ethernet
interface ethernet 0/3
  ip address 20.1.1.1 255.255.255.0
  aaa
    exit aaa
  qos
    module
      exit module
    chassis
      exit chassis
    exit qos
  exit ethernet
interface ethernet 0/4
  ip address 30.1.1.1 255.255.255.0
  aaa
    exit aaa
  qos
    module
      exit module
    chassis
      exit chassis
    exit qos
  exit ethernet
interface console
```

```
  aaa
    exit aaa
  exit console
gvrp
  exit gvrp
snmp-server
  engine-id
    local 0000000c000000007f000001
    exit engine-id
  chassis-id SR
  enable traps
    exit traps
  exit snmp-server
rmon
  exit rmon
oam
  cfm
    enable
    ethtype 88e6
    exit cfm
  exit oam
icmp_timestamp
telnet_banner
  exit telnet_banner
sntp
  exit sntp
ip proxy-dns
  exit proxy-dns
ip load-balancing per-flow
ipv6 unicast-routing
ipv6 load-balancing per-flow
mpls tunnel-mode uniform
firewall global
  algs
    dns
      exit dns
    exit algs
  max-connection-limit self 2048
  exit firewall
firewall internet
  exit firewall
firewall corp
  policy 1024 out permit
    exit policy
  exit firewall
dst
  no enable
  exit dst
```

5.7.2.1. running-config:

begin:

```
SR# show running-config begin interface
Retrieving configuration... please wait

interface ethernet 0/1
  ip address 192.168.90.2 255.255.192.0
  aaa
    exit aaa
  qos
    module
      exit module
    chassis
      exit chassis
    exit qos
  exit ethernet
interface ethernet 0/2
  ip address 10.1.1.1 255.255.255.0
  aaa
    exit aaa
  qos
    module
      exit module
    chassis
      exit chassis
    exit qos
  exit ethernet
interface ethernet 0/3
  ip address 20.1.1.1 255.255.255.0
  aaa
    exit aaa
  qos
    module
      exit module
    chassis
      exit chassis
    exit qos
  exit ethernet
interface ethernet 0/4
  ip address 30.1.1.1 255.255.255.0
  aaa
    exit aaa
  qos
    module
      exit module
    chassis
      exit chassis
    exit qos
  exit ethernet
interface console
  aaa
    exit aaa
  exit console
gvrp
  exit gvrp
snmp-server
  engine-id
    local 0000000c000000007f000001
    exit engine-id
  chassis-id SR
  enable traps
    exit traps
  exit snmp-server
rmon
```

```
  exit rmon
oam
  cfm
    enable
    ethtype 88e6
    exit cfm
  exit oam
icmp_timestamp
telnet_banner
  exit telnet_banner
sntp
  exit sntp
ip proxy-dns
  exit proxy-dns
ip load-balancing per-flow
ipv6 unicast-routing
ipv6 load-balancing per-flow
mpls tunnel-mode uniform
firewall global
  algs
    dns
      exit dns
    exit algs
  max-connection-limit self 2048
  exit firewall
firewall internet
  exit firewall
firewall corp
  policy 1024 out permit
    exit policy
  exit firewall
dst
  no enable
  exit dst
```

As can be seen, all the configurations prior to “interface ethernet 0/1” are skipped.

include:

```
SR# show running-config include interface
Retrieving configuration... please wait

interface ethernet 0/1
interface ethernet 0/2
interface ethernet 0/3
interface ethernet 0/4
interface console
```

As can be seen, all the configurations matching interface are displayed.

exclude

```
SR# show running-config exclude interface
Retrieving configuration... please wait

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
    module voip-gwy local0 none
    exit syslog
  exit logging
hostname SR
log utc
event
  exit event
terminal
  exit terminal
qos
  module
    exit module
  chassis
    exit chassis
  exit qos
module serial 1/1
  exit serial
module serial 1/2
  exit serial
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
  ip address 192.168.90.2 255.255.192.0
  aaa
    exit aaa
  qos
    module
      exit module
    chassis
      exit chassis
    exit qos
  exit ethernet
  ip address 10.1.1.1 255.255.255.0
  aaa
```

```
    exit aaa
  qos
    module
      exit module
    chassis
      exit chassis
    exit qos
  exit ethernet
  ip address 20.1.1.1 255.255.255.0
  aaa
    exit aaa
  qos
    module
      exit module
    chassis
      exit chassis
    exit qos
  exit ethernet
  ip address 30.1.1.1 255.255.255.0
  aaa
    exit aaa
  qos
    module
      exit module
    chassis
      exit chassis
    exit qos
  exit ethernet
  aaa
    exit aaa
  exit console
gvrp
  exit gvrp
snmp-server
  engine-id
    local 0000000c000000007f000001
    exit engine-id
  chassis-id SR
  enable traps
    exit traps
  exit snmp-server
rmon
  exit rmon
oam
  cfm
    enable
    ethtype 88e6
    exit cfm
  exit oam
icmp_timestamp
telnet_banner
  exit telnet_banner
sntp
  exit sntp
ip proxy-dns
  exit proxy-dns
ip load-balancing per-flow
```

```
ipv6 unicast-routing
ipv6 load-balancing per-flow
mpls tunnel-mode uniform
firewall global
  algs
    dns
      exit dns
    exit algs
  max-connection-limit self 2048
  exit firewall
firewall internet
  exit firewall
firewall corp
  policy 1024 out permit
    exit policy
  exit firewall
dst
  no enable
  exit dst
```

As can be seen, all the configurations which are not matching interface have been displayed.

include-section

```
SR# show running-config include-section interface
Retrieving configuration... please wait

interface ethernet 0/1
  ip address 192.168.90.2 255.255.192.0
  aaa
    exit aaa
  qos
    module
      exit module
    chassis
      exit chassis
    exit qos
  exit ethernet
interface ethernet 0/2
  ip address 10.1.1.1 255.255.255.0
  aaa
    exit aaa
  qos
    module
      exit module
    chassis
      exit chassis
    exit qos
  exit ethernet
interface ethernet 0/3
  ip address 20.1.1.1 255.255.255.0
  aaa
    exit aaa
  qos
    module
      exit module
    chassis
      exit chassis
    exit qos
  exit ethernet
interface ethernet 0/4
  ip address 30.1.1.1 255.255.255.0
  aaa
    exit aaa
  qos
    module
      exit module
    chassis
      exit chassis
    exit qos
  exit ethernet
interface console
  aaa
    exit aaa
  exit console
```

As can be seen, it displays those configurations that match interface. In addition, configurations which are part of the tree of the interface configurations are also displayed.

exclude-section

```
SR# show running-config exclude-section interface
Retrieving configuration... please wait

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
    module voip-gwy local0 none
    exit syslog
  exit logging
hostname SR
log utc
event
  exit event
terminal
  exit terminal
qos
  module
    exit module
  chassis
    exit chassis
  exit qos
module serial 1/1
  exit serial
module serial 1/2
  exit serial
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
gvrp
  exit gvrp
snmp-server
  engine-id
    local 0000000c000000007f000001
    exit engine-id
  chassis-id SR
  enable traps
    exit traps
  exit snmp-server
rmon
  exit rmon
oam
  cfm
    enable
    ethtype 88e6
    exit cfm
  exit oam
icmp_timestamp
telnet_banner
  exit telnet_banner
sntp
  exit sntp
ip proxy-dns
  exit proxy-dns
ip load-balancing per-flow
ipv6 unicast-routing
ipv6 load-balancing per-flow
mpls tunnel-mode uniform
firewall global
  algs
    dns
      exit dns
    exit algs
  max-connection-limit self 2048
  exit firewall
firewall internet
  exit firewall
firewall corp
  policy 1024 out permit
```

```
    exit policy
  exit firewall
dst
  no enable
  exit dst
```

As can be seen, only those configurations that do not match interface are displayed. In addition, configurations which are not part of the tree of the interface configurations, are also displayed.

5.7.2.2. startup-config

Similarly we have the commands:

```
SR/file# show startup-config file system.cfg begin interface
SR/file# show startup-config file system.cfg include interface
SR/file# show startup-config file system.cfg exclude interface
SR/file# show startup-config file system.cfg include-section interface
SR/file# show startup-config file system.cfg include-section interface
```

5.7.2.3. Other examples

Suppose we want to match the command "interface ethernet 0/1":

```
SR# show running-config include interface ethernet 0/1
OR
SR# show running-config include interface
OR
SR# show running-config include ethernet
OR
SR# show running-config include 0/1
OR
SR# show running-config include ethernet 0/1
```

6. Problems Resolved since the 10.3.4.15 Release

Bug Reference	Description
wi01089340	SR2330 crashes intermittently in OSPF as internal TCP IPC packets between routing tasks were timing out and the socket was closed.
wi01071727	Secure Router as firewall runs out of memory disrupting network connections.
wi01078834 wi01126510	When "show arp" command is executed on Secure Router, a semaphore deadlock occurs between two tasks causing temporary outages on the router.
wi01095185 wi01107703	With more than 100 phones terminating Contivity VPN connections on Secure Router, the router crashes and needs a reboot.
wi01101567	11xx phones get dropped from VPN connection on SR2330. During phase1 negotiation, the 11xx phones change the source port of messages and SR uses the source port as seen in the first received message of negotiation. This causes the message to be not received from 11xx phones and leads to failure in setting up VPN connection.

wi01070630	TACACS Server shuts down user account due to Secure Router sending the same bad password multiple times for the same user.
wi01068444	SR4134 forwards Check Point HA packets causing a network flood.
wi01059357	NMAP scan on Secure Router kills telnet requiring a reboot to recover.
wi01094132	Under heavy traffic load, SR has OSPF adjacency flap and upon OSPF neighbor going to FULL, the router crashes.
wi01092498	VPN clients unable to connect to Secure Router intermittently as the connection tables were exhausted due to abnormally terminated sessions, thus not allowing genuine clients to setup new sessions.
wi00537014	Management access for SecureID.
wi00537018	Ability to disable telnet client.
wi00537032	Change VRRP preempt default to disabled.
wi00537175	16 user level accesses using TACACS server authorization.
wi00537860	Avaya VPN Client unable to connect - firewall internet self policy issue.
wi00538053	SNMP ifIndex not persistent if config changes then reboot.
wi00538140	SR 2K/4K using deprecated BGP traps.
wi00538144	No HDLC Channels available for channel 20 and higher on 8-port E1 module.
wi00538212	After several FTP sessions through the NAT enabled firewall on SR, FTP transaction fails.
wi00538216	Crash in QOTD task when password hack is attempted.
wi00538225	Crash when DHCP server enabled with lag interface.
wi00538239	Constant reboots with tDhcpsTask crash.
wi00538242	Automatically adding published ARP entries for non-self NAT-IP Policies.
wi00538274	Intermittent outage of internet access through NAT enabled firewall on SR.
wi00538205	Point to Point Tunnel Protocol (PPTP) connection to server not working with FW.
wi00538286	ICMP checksum incorrect.
wi00552711	Dropped packets not shown when using frame relay.
wi00552879	Intermittent telnet connection hang to VRRP IP address.
wi00553087	Unable to monitor the router using SNMP when IPIP tunnel involved.

wi00553106	RIP/OSPF fails on tunnel in specific scenario.
wi00553114	Router locked up when run command into SSH session via Radius.
wi00553140	SR 4K crashed when policy is entered.
wi00553143	Latency issues on 64 kbps links.
wi00553149	NSM Task crash on 4K on soak setup.
wi00553187	Fan RPM showing as 0.
wi00553204	Management Information Base MIB Object Speed is displayed as Zero when it should be line speed.
wi00553235	Telnet and console hang.
wi00554792	Crash when doing config then write memory.
wi00653615	DHCP pool name > 8 characters in length causes error.
wi00653632	Crash in zNSM when OSPF Ethernet interface bounces.
wi00653637	User name is absent in voice call made through ISDN PRI(QSIG) on SR2330.
wi00653660	Default route not put into routing table.
wi00653662	Crash in telco statistics processing in heavily utilized system.
wi00653687	VPN client fails when static-default route used out untrusted interface.
wi00653730	Unable to save config/show run after clear all-user-sessions.
wi00703978	Ping trace route show * on a good link is broken.
wi00775000	SNMP traps are not using configured trap-source as the IP source in traps.
wi00817023	When an Avaya VPN Client is behind NAT, after IPsec rekeying, unsolicited traffic from corp to client carries dest port as "0".
wi00825493	show tech causes all OSPF neighbors to drop.
wi00826290	Intermittent Crash in rxPoll.
wi00826763	Intermittent Crash in tStrmTask.

7. Known issues

Bug Reference	Description
wi00538238	SLA:udp-jitter profiles - Source does not transmit packets to the reachable destination.
wi00815571	SSM crashes in attendant call transfer scenario with 1120 phone in backup mode.
wi00821695	Incoming call on ISDN for DMS100 switch does not accept Setup with PI.
wi00822647	Outgoing BRI calls do not work with NTT setup.
wi00825593	SCS interop: Call redirection (forward no answer) – no PRACK for 180 ringing.
wi00825634	SCS interop: Blind transfer does work when transferee and transfer target are both PSTN ISDN (BRI) subscribers.
wi00826286	The IPsec policy **`pfs-group`** command has an option for configuring Group 16 (4096–bit). However the Secure Router does not support this option.
wi00826296	The certificate authority trustpoint key pair for **`dsa`** has an option for configuring `2048`, `3072`, and `4096` key sizes. However the Secure Router does not support those key sizes.
wi01070392	After saving the configuration and rebooting, the 44 Gig card fails to come up with the saved configuration. This happens only when there is no user name configured and with the display mode set to MIN. **Workaround:** Configure a user name and set the display mode to MAX.
wi01076530	There is a delay of approximately 30 seconds before IPSLA displays the static route tracker's current Up/Down status.
wi01076726	Under **firewall global** > **object**, you can use `address <object-name> <ipaddress>` to configure multiple objects for a **range of IP addresses** or **subnets** depending on the subnet mask you enter. The router interprets `255.255.0.0` mask as a range and `16` as a subnet. For example, `address OFT 47.10.64.0 255.255.0.0` is treated as a range of addresses and `address OFT 47.10.64.0 16` as a subnet.
wi01077215	IPFIX does not capture traffic flowing through a LAG interface.
wi01082681	IPFIX ingress flows are not monitored when the interface is part of the firewall.
wi01088425	IPFIX supports monitoring VLANs in Access Port mode only. It does not support other modes such as Trunk, Hybrid, and LAG modes.

8. Outstanding Issues

N/A

9. Known Limitations

9.1. IPFIX

9.1.1. IPFIX ingress flows will not be monitored with firewall enabled on the interface.

9.1.2. IPFIX is not supported over LAG interfaces and VLANs in Trunk and hybrid modes.

9.2. IPSLA:

- IPV6 static routes with SLA monitor is not supported
- Profile Operation “modify” is not allowed once configured. The only way is to delete and recreate the profile because other attributes for profile like threshold-type, threshold-value and action are all dependent on the operation.
- There will be a delay of approximately 30 seconds in the displaying Tracker’s Up/Down status.

9.3. CPU traps "total” and “process" are not enabled with the cli "enable traps enable-all". They need to be enabled individually.

9.4. While configuring IPSEC objects:

9.4.1. When dotted decimal notation format is used for specifying subnet prefix instead of integer format, it will be considered as the range of ip-address.

Example: address OFT 10.64.0.0 255.255.0.0

9.4.2. Using the address object defined in that format with IPSEC policy, the network subnets to be secured will be validated for the source network range starting from 10.64.0.0 to 255.255.0.0 instead of just 16-bit prefix length match of 10.64.0.0 network.

9.5. The global firewall option “reset-invalid-acks” has been deprecated. The command is still recognized but will have no effect.

9.6. The VPN Client passwords on the 11xx Phones are case sensitive and must be entered in lower case only on the phone. This affects only the 11xx phones. The 96xx phones and PC VPN Client handle client passwords properly.

10. Documentation Corrections

The following documents have been updated with changes to reflect the latest software. These documents are available at http://www.avaya.com/support.

- NN47263-302: Commissioning
- NN47263-500: Configuration - WAN Interfaces
- NN47263-501: Configuration - Layer 2 Ethernet
- NN47263-502: Configuration - IPv4 and Routing
- NN47263-504: Configuration - IPv4 Multicast Routing
- NN47263-507: Command Line Reference
- NN47263-508: Configuration - SIP Media Gateway
- NN47263-510: Configuration - SIP Survivability
- NN47263-600: Security - Configuration and Management
- NN47263-602: Configuration - Network Management
- NN47263-700: Troubleshooting
- NN47264-302: Commissioning (AG)
- NN47264-501: Configuration - Ethernet (AG)
- NN47264-507: Command Line Reference (AG)
- NN47264-508: Configuration - SIP Media Gateway (AG)

11. Additional Notes

The IKE NAT ALG (application level gateway) was always enabled in prior releases. This caused a number of issues with IKE NAT Traversal. The IKE NAT ALG is now enabled and disabled by the enable for the IKE firewall ALG, under the global firewall configuration. Both the Firewall and NAT ALGs are disabled by default and enabled or disabled in unison by this one control.

Avaya recommends that the maximum active encrypted VPN sessions with the Secure Router 4134 do not exceed 300. You can configure up to 1000 encrypted VPN sessions.

The Secure Router 2330 maximum active encrypted VPN sessions is 100.

Notice

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

Copyright

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