Secure Router 3120/ Secure Router 1000 Series

Software Release 9.4.2 ReadMe

1. Release Summary

Release Date: Aug 17, 2012
Purpose: Software maintenance release to support the Secure Router product.

2. Notes for Upgrade of Secure Router

Please see the technical documentation for the Secure Router 3120 and 1000 Series version 9.4.x. available at: http://www.avaya.com/support for details on how to upgrade your Secure Router unit.

3. Secure Router Product

Description	File Size	Version	File Name
Secure Router 1001 Application Image	9 420 775	9.4.2	J1100.Z
Secure Router 1001S Application Image	9 872 137	9.4.2	JP1010.Z
Secure Router 1002/1004 Application Image	8 751 650	9.4.2	T1000.Z
Secure Router 3120 Application Image	9 523 276	9.4.2	H1000.Z

4. Version of Previous Release

Software Version 9.4.1

5. New Features in the 9.4.2

5.1 Ability to configure whether to update the TOS field of VLAN header

The default behavior is to leave the TOS field unchanged on the VLAN header when forwarding packets. There is a new CLI command to change the router to always update the TOS field with the QOS DSCP value and it takes effect immediately and does not require the router to be rebooted.

5.1.1 Cli Commands

5.1.1.1 system tos-field-update

This command changes the router to copy the QOS DSCP value into the TOS field of the VLAN header. The no option resets the router back to the default behavior of not copying the QOS DSCP value when forwarding packets.

Syntax

[no]system tos-field-update

Example:

host/configure# system tos-field-update

5.1.1.1 show qos tos-field-update

This command shows whether the TOS field will be updated on the VLAN header with the QOS DSCP value.

Syntax

show qos tos-field-update

Example:

```
host# show qos tos-field-update

QOS VLAN Forwarding Behavior
 --------------------------
Do not copy the QOS DSCP value into the TOS field in the VLAN header
 host#
```

5.2 Packet Capture of VLAN Packet with Filter Rules

A new access-list rule type was added to support capturing packets related to the MAC portion of the packet including specific VLAN ID. The new rule type is called mac and it **only** filters the MAC portion of the packet header. The MAC accesss-list can filter on the source and destination MAC address, Ether type, CoS user defined field, VLAN and second VLAN.

WARNING

The access rules will first filter on all the MAC rules and then filter the protocol rules. The MAC rules can only filter the MAC portion of the packet and the protocol rules (ip,icmp,tcp,udp) can only filter on the packet above the MAC header.

mac access-list rule syntax:
add permit mac <src-mac> <dest-mac> [<ethertype>] [<cos>] [<vlan>][<vlan2>]

The following table describes the access-list rule parameters.

Table 1: Access rule parameter definitions

Name	Description	Value	Rule Type
source	source mac/IP address	Dot notation or any	MAC,ICMP,IP,UDP,TCP
destination	destination mac/IP address	Dot notation or any	MAC,ICMP,IP,UDP,TCP
ethertype	mac Ether Type	Hexadecimal 4 digit	MAC
cos	mac class of service	0-7	MAC
vlan	mac vlan id	1-4096	MAC
vlan2	mac inner vlan id for double tag	1-4096	MAC
sport	source port	0- 65535	UDP,TCP
dport	destination port	0- 65535	UDP,TCP
icmptype	ICMP type	0-255	ICMP
icmpcode	ICMP code value	0-255	ICMP
precedence	IP precedence	0-7	IP,UDP,TCP
tos	IP type of service	0-16	IP,UDP,TCP
flags	TCP flags	fin,rst,psh,syn,urg,ack	TCP

The following example show the configuration required to capture all the TCP traffic over VLAN ID 10 with an ethertype of 0x8100 on bundle WAN.

```
Host/debug/pcap > show-config
Packet capture global configurations:
====================================
Maximum size reserved for packet capture : 5120KB
Alloted for packet capture sessions : 0KB
Available for packet capture sessions : 5120KB
Maximum number of sessions allowed : 5
capture configuration session interface: buffer size total pkts
name : committed : active : (Kb) : captured :
================================================================================
Host/debug/pcap > access-list vlan10
Host/debug/pcap/access-list vlan10 > add permit  mac any any ethertype 0x8100 vlan10
Host/debug/pcap/access-list vlan10 > add permit tcp any any

Host/debug/pcap > capture wan
Host/debug/pcap/capture wan > attach bundle WAN
Host/debug/pcap/capture wan > filter vlan10 in
Host/debug/pcap/capture wan > filter vlan10 out
Host/debug/pcap/capture wan > wrap
```

```
Host/debug/pcap/capture wan > direction both
Host/debug/pcap/capture wan > commit
Host/debug/pcap/capture wan > show-config
Packet Capture :wan
====================================
Interface attached : WAN
State : Disabled.
Configurations committed
Duration of session : 0 secs
Direction : IN, OUT
Buffer Wrap : ON
Capture all packets
Capture entire contents of each packet
Capture non-IP packets : ON
packets captured in this session : 0
Buffer size for this session : 1024KB
Inbound Filter : vlan10
Pcap Filter Rule List : vlan10
1. permit mac any any  ethertype 0x8100 vlan 10
2. permit tcp any any
Outbound Filter : vlan10
Pcap Filter Rule List : vlan10
1. permit mac any any  ethertype 0x8100 vlan 10
2. permit tcp any any
Host/debug/pcap/capture wan > exit
Host/debug/pcap > show-config
Packet capture global configurations :
====================================
Maximum size reserved for packet capture : 5120KB
Alloted for packet capture sessions : 1024KB
Available for packet capture sessions : 4096KB
Maximum number of sessions allowed : 5
capture configuration session interface: buffer size total pkts
name : committed : active : (Kb) : captured :
================================================================================
wan yes no WAN 1024 0
================================================================================
Host/debug/pcap > enable
Enabled session vlan10
Host/debug/pcap > show-config
Packet capture global configurations :
====================================
Maximum size reserved for packet capture : 5120KB
Alloted for packet capture sessions : 1024KB
Available for packet capture sessions : 4096KB
Maximum number of sessions allowed : 5
capture configuration session interface: buffer size total pkts
name : committed : active : (Kb) : captured :
================================================================================
wan yes yes WAN 1024 128
================================================================================
Host/debug/pcap > no enable
```

6. Compatibility

N/A

7. Problems Resolved in the 9.4.2 Release

Bug Reference	Subsystem	Description
wi00532730	Platform	CT3 module LEDs display is incorrect in show AIS/STAT
wi00839233	PPPOE	NAT policy specified with a PPPOE interface name errors when the system.cfg is read in on reboot.
wi00853549	Multicast	Multicast stops working after 18 bundles
wi00871403	IPSEC	RxPoll crash
wi00924994	ARP	DHCP Relay marking ARP Entries permanent in certain conditions
wi00981934	QOS	After upgrading to 9.4.1 from 9.3.2, DSCP now gets marked to 802.1p, even without QOS configured
wi01003202	VLAN	VLAN Bridging mode a MAC address will be learned on the wrong port very infrequently
wi01011050	BGP	Router rebooted and the event log contained the message "`Assertion failed gated[tGateDTask]: file "bgp_sync.c", line 1088`

8. Outstanding Issues

Refer to the previous Release Notes.

9. Known Limitations

Refer to the previous Release Notes

10. Documentation Corrections

- The section "Packet Capture of VLAN Packet with Filter Rules" in Chapter 47 "Configuring Packet Capture" in both the Ayava Secure Router 3120 Configuration Guide version 9.4 doc id NN47260-501, 02.01 and Ayava Secure Router 1000 Configuration Guide version 9.4 doc id NN47262-501, 02.01 is incorrect and has been corrected in the release notes under New Features.

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
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