VYATTA, INC. | Release Notes

Vyatta Release 2.0

February 2007

Document Part No. A0-0081-10-02

Vyatta
Suite 160
One Waters Park Drive
San Mateo, CA 94403
vyatta.com

Contents

New in This Release

- **IPsec VPN**. This release introduces support for IPsec VPN. This IPsec VPN implementation allows small to large enterprises and enterprise branch offices to deploy a high-performance, robust, integrated routing and security solution for site-to-site secure communications. Vyatta's implementation employs standard cryptographic and hash algorithms and is interoperable with other standards-based IPsec VPN products.
- **Bug fixes.** A number of issues have been resolved with Release 2.0. A summary list of these is provided in the "Resolved Issues" section, which begins on page H2.

Behavior Changes

There are no behavior changes in this release.

Upgrade Notes

Release 1.1.2 can be upgraded to Release 2.0 using an ordinary package upgrade.

Release 2.0 configuration files are not compatible with configuration files from Release 1.0.3 and earlier. Therefore, existing configurations from Release 1.0.x must be migrated to the new release. Users are strongly urged to consult the Release 2.0 upgrade procedure available in the Subscription Knowledge Base located on the Vyatta Customer Care Center web site (http://www2.vyatta.com/support) for instructions on how to most easily migrate existing Release 1.0.x configurations to Release 2.0.

Resolved Issues

Bug ID	Component	Severity	Description
89	CLI	critical	XORP 157: changing date/time causes Process Failure
627	BGP	major	XORP 439: Incorrect functioning of BGP in state OpenSent
904	System	major	Add drive size display to install-system:select_drive()
1018	System	minor	install-system complains about deleting partitions that don't exist
1177	System	major	Installer: prompts should accept lowercase and shorter responses
1178	System	major	Installer: installation fails when unexpected input is encountered
1179	System	major	Installer: auto partitioning option should default to the whole drive
1180	System	major	Installer: specifying a larger root partition than the install drive aborts the installer
1438	CLI	minor	"show hardware [cpu | mem | pci]" are all available to both user “vyatta” and user “root”; however, "show hardware dmi" only works for the root user.
1498	NAT	critical	NAT - add ip_conntrack_ftp and ip_nat_ftp modules
1578	VRRP	major	Interface deletion - Related VRRP data need to be removed
1584	System	unassigned	Partition mis-spelled in install script
1585	System	major	This will destroy all data section of install script does not take "No" for an answer
1589	GUI	unassigned	FW - GUI: "Show Firewall": parser error
1607	GUI	unassigned	Strike-through under Show Processes
1609	Documentation	unassigned	Frame-Relay interface configuration example incorrect
1617	System	minor	Install script should error when drive size is smaller than allowable capacity
1618	System	enhancement	Install script root image minimum size should be decreased
1620	System	major	Create a method to preserve interface numbering

			information in config partition
1621	OSPF	unassigned	Configurable adaptive subsecond SPF delay for OSPF
1622	OSPF	major	Random LSA refresh timers
1655	System	minor	Config Partition Mounted as ext2 - ext2_fill_super: mounting ext3 filesystem as ext2
1658	Documentation	critical	Documentation recommends configuring 127.0.0.1/30 on interface loopback lo
1670	System	trivial	Excessive PCI / IRQ messages during boot on MSI systems
1695	Interfaces	critical	interfaces are not automatically pre-populated in the config

Known Issues

Bug ID	Description
482	Load configuration fails if policy is applied as import or export. This problem occurs if a user has an existing configuration that includes a protocol configuration with a policy applied (import or export). If the user tries to load a configuration that does not include that protocol, the "load" command fails. Vyatta recommends avoiding the use of the “load” command as there are several serious problems with this command at this time.
569	OSPF NSSA does not originate AS-external-LSA (TC 3.2.6.3.2). If the router is configured with one interface (for example, eth0) in the backbone area and one interface (for example, eth1) in the NSSA area, and it learns Type-7 LSA from a neighbor in the NSSA area, the router does not correctly originate AS-external-LSAs to its neighbors in area 0.0.0.0.
713	Help may incorrectly indicate commands as executable. For example, the date ntp command is not executable without an additional parameter, but the help shows that <Enter> is an option.

886	OSPF - summary-LSA deleted if area-range with same base subnet deleted. If a user configures OSPF with 2 interfaces, one in the backbone area and one in a non-backbone area in different areas and interface in the non-backbone area does not have any neighbors, the network of the interface is correctly advertised as a summary-LSA. If the user then adds an "area-range" with the same base subnet, the new summary-LSA does not have an incremented sequence number, but does have a new LSA age, so the LSA is considered invalid by its peers.
1021	Create "default-lsa" node for area-type stub and NSSA. When a user creates an area and sets its area-type to "stub" or "nssa" the default LSA is not advertised until the user also creates the "default-lsa" node. This is confusing as many other routers automatically announce the default LSA when they have an area-type of stub or nssa. This bug has been filed with the XORP project as bug number 605.
1084	Serial - PPP authentication (PAP & CHAP) do not work. If a serial interface is configured with either PAP or CHAP the interface never tries to authenticate PPP sessions. If a remote side is configured with authentication the session fails to establish until the authentication is removed. This bug has been filed with Sangoma as bug number 487.
1113	Update help for "save" and "load". Currently the help for "save" and "load" does not provide the list of valid options (file, tftp, ftp, http) and the proper syntax for each of these options. The syntax options are as follows: • Absolute path • Relative path. Relative paths interpreted relative to the path configured in the "config-directory" parameter of the "rtrmgr" configuration node. • TFTP server. The syntax is tftp://*ip-address*/*config-file.* • FTP server. The syntax is ftp://*ip-address*/*config-file.* If you use FTP, you will be prompted for a user name and password. • HTTP server. The syntax is http://*ip-address*/*config-file.* Note that subdirectories for TFTP, FTP, and HTTP servers are not supported at this time, due to bug number 1124.
1124	Save targets that are URL (tftp, etc.) do not support sub-directories. Currently the URL cannot contain sub-directories such as tftp://*servername*/sub-1/*config.file*. The only supported capability is tftp://*servername*/*config.file*.
1201	Setting serial interface to ignore Cisco HDLC keep-alives does not work. If a Sangoma interface is configured with a Cisco HDLC transmit keep-alive value, the Sangoma interface transmits keep-alives every 6 seconds, regardless of the configured value. This bug has been filed with Sangoma as bug number 486.
1231	"show interfaces ethernet eth*x* vif ?" shows *all* configured vifs. This option should return only vifs configured for the specified interface.

1289	Package removal fails. The system does not allow the user to remove a package that is designated as "essential," including packages on which "essential" packages depend. This can prevent removal of unwanted packages. This feature is there to preserve the stability and integrity of the system, but can be confusing because the error messages are not always clear.
1354	Changes from CLI being transmitted to GUI. This problem occurs if there are multiple users, some logged on to the CLI and some to the GUI. If a user logged on to the CLI commits a configuration change, then the "Commit All Changes" button of the GUI changes to yellow, which ordinarily signals that there are uncommitted changes. In any case, the GUI state should not reflect changes by CLI users. In general, Vyatta recommends that only a single user configure the system at a given time.
1413	SNMP walk of system fails with BGP configured. With BGP configured and a full routing table, a SNMP walk of the system hangs. The SNMP agent will not then respond to further queries. Without BGP configured, a full SNMP walk succeeds.
1415	Excessive CPU use by SNMP agent. When SNMP is configured with BGP and a full routing table, the SNMP agent uses an unexpectedly high amount of CPU. Excessive CPU usage increases with the number of routes in the routing information base.
1484	"show interfaces serial wan0 ppp" shows PAP and CHAP disabled when they are enabled. The Sangoma card incorrectly reports results to the router command shell, causing the router command to return incorrect results for PAP and CHAP. This bug has been filed with Sangoma as bug number 1075.
1501	Default config directory should be created on configuration. If the user configures a new default configuration directory (by modifying the "config-directory" attribute of the "rtrmgr" configuration node), the change is accepted. However, subsequently saving configuration will cause an error, as the router cannot write to the new directory. Work-around: Login as root and create the directory from the bash prompt, by typing **mkdir** */path-to-directory/directory*
1540	CLI: Options that require root access should be hidden for other users. If a user is logged on to the CLI as a non-root user, commands requiring root access appear to be available. However, if the user attempts to execute the command, it fails with a number of error messages. These commands should either be hidden from non-root users, or else the command should fail with a message clearly specifying that root permissions are required.

1551	Receive "102 Command failed delete policy" when attempting to delete a policy that was bound to a non-existent protocol. This error can occur if the user deletes a protocol configuration node (such as OSPF) that has an export policy applied. Once the protocol has been deleted, an attempt to delete the associated policy generates an error. This issue clears on reboot.
1631	When a firewall is removed from an interface, iptables still shows the chain attached to that interface.
1636	SNMP module for BGP does not build. This error means that SNMP queries cannot be made to the BGP MIB.
1662	CLI: Error editing multi-node. The system does not always register multi-nodes correctly when created using the “set” command. Subsequent to setting the multi-node, the [edit] prompt may not correctly track the user’s location in the configuration tree.
1669	VPN: "show route" inconsistent with "show route system forward". When a remote subnet is specified in tunnel configuration, the IPsec process adds a static route to the remote subnet to the Forwarding Information Base (FIB). The XORP process is not aware of this route, and does not report it in the output of the “show route” command. However, the “show route system forward” command, which shows all routes in the FIB, does report this route. Therefore, the information shown by these two commands will be inconsistent in this case.
1682	VPN configuration changes should not restart ipsec. Currently, changing any IPsec VPN parameter causes the IPsec process to restart. This results in all existing tunnels being torn down and re-established.
1704	Duplicate ESP SAs are being created with auto=start. The issue occurs if the tunnel connection is set “auto=start” on both sides. Once the IPsec process has started on both sides, the peers come up and negotiate an ISAKMP SA, then they negotiate an ESP SA, then a few seconds later they negotiate another ESP SA. Based on the byte counters for the SA it appears that the second set of negotiated SAs is the one used. If one end of the tunnel connection is set to "auto=add" and the other left to "auto=start" then one pair of SAs is created, as expected.
1713	OFR fails to bring up VPN tunnel automatically after remote site reboot. When a VPN tunnel is established between the OFR and a Cisco router, the tunnel on the OFR must also be restarted when the Cisco router is reloaded. To restart OFR tunnels, you can commit a configuration change for any IPsec VPN parameter, or you can log on to the OFR Linux command prompt as user “root” and issue the **ipsec setup restart** command. Either action restarts all OFR tunnels.

1714	OFR fails to bring up VPN after remote site SA deletion (and notify). When a VPN tunnel is established between the OFR and a Cisco router, the tunnel on the OFR must be re-established when the security association is deleted on the Cisco router. To restart OFR tunnels, you can commit a configuration change for any IPsec VPN parameter, or you can log on to the OFR Linux command prompt as user "root" and issue the **ipsec setup restart** command. Either action restarts all OFR tunnels.
1734	VPN: NAT Traversal doesn't work with NETKEY implementation of OFR. When an IPsec VPN tunnel traverses a NAT device, the VPN gateway where the tunnel terminates is unable to decrypt the packet, even though the IPsec has been successfully established by both peers. Note that this problem occurs only if the VPN tunnel traverses through the NAT device. An OFR can be operated as both a NAT device and a VPN tunnel termination without a problem.
1738	VPN: "show vpn ike sa" should only show 1 entry per peer. Currently, this command may display multiple entries per peer.