VYATTA, INC. | Release Notes

Vyatta Release 6.5R1

October 2012

Document Part No. A0-0095-10-41

Vyatta
1301 Shoreway Road
Suite 200
Belmont, CA 94002
vyatta.com

Contents

These release notes document changes made for the Vyatta Release 6.5R1. These release notes include the following sections:

Security

This release resolves the following security bulletins:

- CVE-2012-3955 - Reducing the expiration time for an IPv6 lease may cause the server to crash. Resolved with Bug ID 8367.
- CVE-2012-2141 - Incorrect agent index can crash SNMP. Resolved with Bug ID 8080.

New Features in This Release

- **Virtual tunnel interfaces.** This release introduces virtual tunnel interfaces (VTIs). A VTI provides a termination point for a site-to-site IPSec VPN tunnel and allows the IPsec tunnel to behave like other routable interfaces. In addition to simplifying IPsec configuration, a VTI enables many common capabilities to be used with IPsec because the VTI endpoint is associated with an actual interface. VTIs are described in the *Vyatta VPN Reference Guide.*
- **BGP multipath support.** This release adds support for BGP multipath. BGP multipath allows for multiple paths to a given destination. This permits traffic load to be shared across the paths, allowing use of network resources that might otherwise be used only as backup.

- **VRRP operational command changes.** VRRP operational mode commands have been updated to be more efficient and work in a consistent manner. Also, the **show vrrp** command output has been reformatted and reorganized for easier viewing. VRRP features are described in the *Vyatta High Availability Reference Guide.*
- **IPsec for IPv6.** The Vyatta system's IPsec functionality has been extended to IPv6 and existing commands for IPsec VPNs have been updated to support IPv6 addressing and options. IPsec functionality is described in the *Vyatta VPN Reference Guide.*
- **Policy-based routing.** This release of the Vyatta system allows you to define IPv4 and IPv6 routing policies to classify and differentially process traffic based on classification. Traffic can be classified according to a number of different attributes, including source and destination address and port, protocol, ICMP or ICMPv6 type, packet fragmentation, IPsec packet, or TCP flag. Traffic matching classification rules can be dropped, marked, modified, or sent to an alternative routing table. Policy-based routing is described in a new guide, the *Vyatta Policy-Based Routing Reference Guide.*
- **Hyper-V® hypervisor.** The Vyatta system now supports for the Microsoft® Hyper-V hypervisor. Like other Vyatta-supported virtualization platforms, Hyper-V allows multiple Vyatta virtual machines to be run simultaneously on the same hardware platform. Instructions on installing and upgrading the Vyatta system on a Hyper-V system are provided in the new *Vyatta Installing and Upgrading: Hyper-V.* At this time, the Vyatta system has only been fully tested on Hyper-V 2008, and not on Hyper-V 2012.
- **64-bit system image.** Vyatta now provides a 64-bit system image in addition to the 32-bit image. In addition to 64-bit support for physical hardware, a 64-bit virtualization version with templates for VMware, XenServer, Amazon Web Services AMI, RHEL KVM, and Hyper-V are available.
- **Multiple Ethernet interfaces for AMI.** Previous releases of the Vyatta AMI for Amazon Web Services provided support for only a single Ethernet interface per instance. This version of the system provides support for multiple Ethernet interfaces per instance.
- **QoS Priority Queues.** The QoS capabilities have been extended in this release to include priority queues. This mechanism provides the ability to place traffic matching various criteria into distinct queues, each with a different priority. Traffic is then removed from the queues in priority order – highest priority traffic being transmitted first.

Behavior Changes

- **P2P firewalling functionality deprecated.** In this release, P2P firewalling is deprecated. Support will be completely removed from the Vyatta system in a future release.
- **Serial card support deprecated.** In this release, serial card support is deprecated. Support will be completely removed from the Vyatta system in a future release.

System Limitations

Limitations on SR-IOV virtual function (VF) interfaces. In most cases, the Vyatta system works properly over virtual function interfaces (SR-IOV). However, for some Ethernet network interface cards (NICs) (for example, Intel NICs) in virtual environments where SR-IOV has been enabled, some functionality is not supported. For example, the following is not supported:

- Promiscuous mode: Breaks bridging and reduces packet capture
- Source address: Breaks pseudo-Ethernet and VRRP
- Multiple receive queues: Limits performance

Since these are hardware limitations, the only workaround is to use an alternative connectivity method, such as PCI pass-through, or disable SR-IOV if your hypervisor supports it.

Documentation Changes

Two new documents have been added to the documentation library:

- A new guide has been added to describe installation and upgrade procedures for Vyatta on the Microsoft Hyper-V hypervisor: *Vyatta Installing and Upgrading: Hyper-V.*
- To support policy-based routing, a new guide has been added: the *Vyatta Policy-Based Routing Reference Guide.*

Upgrade Notes

- **Upgrading 64-bit systems.** Changes to the system images in Release 6.5 mean that the “upgrade system image” command will not succeed for systems running a 64-bit virt image. If you are running a 64-bit virt image earlier than Release 6.5, upgrade your system using the “add system image” command.
- **Installing 64-bit systems in virtual environments.** For 32-bit systems, Vyatta produces one ISO image for physical system installations and another, separate, “virt” ISO for virtual system installations. For 64-bit systems, Vyatta produces a single ISO image, which is used for both physical and virtual 64-bit system installations.
- **Kernel version warnings from third-party software.** The Vyatta system uses Linux kernel version 3.0. Some third-party software checks version numbers and mistakenly assumes that version 3.0 differs from the 2.6 kernel series. Kernel version 3.0 is an extension of the 2.6 kernel series. Any warnings related to kernel version can be safely ignored.
- **Upgrading systems using “firewall modify.”** The “firewall modify” functionality is unsupported. The supported equivalent functionality is policy-based routing, introduced in this release. If you are currently using “firewall modify” functionality, be advised that no migration scripts are provided in this release. If you intend to continue using “firewall

modify" functionality, manual migration is required and Vyatta recommends that you upgrade and test your systems in a lab environment prior to going into production. Alternatively, to remove "firewall modify" functionality from your system, first remove the "firewall modify" configuration node from any interfaces on which it is configured. Then remove the "firewall modify" configuration subtree, using the "delete firewall modify" command. Commit and save this configuration change before upgrading to Release 6.5.

- **Double-quote characters in configuration.** If you are upgrading a system that uses the double quote (") character in a value string within the configuration, you must remove the configuration lines containing the double quote character before upgrading. Some such lines can be replaced with functionally equivalent configuration after the upgrade. Failure to do so can render the system inaccessible once it is upgraded.

  The double quote character is sometimes used in free-form text values such as the openvpn-option, DHCP global-parameters and shared-network-parameters, system login banner, and interface description values. Some instances can be worked around using alternate configuration. For example, the configuration:

  ```
  interfaces openvpn vtunX openvpn-option "–push "route 10.254.0.0 255.255.0.0""
  ```

  can be replaced after upgrade with either:

  ```
  interfaces openvpn vtunX openvpn-option "–push route 10.254.0.0 255.255.0.0"
  ```

  or:

  ```
  interfaces openvpn vtunX server push-route 10.254.0.0/16
  ```

  Instances that cannot be worked around must be removed from the configuration prior to upgrading.

CLI Changes

Configuration Mode Parameters	Type of Change	Reason / Comment
interfaces vti <vtix>	Added	VTI
interfaces vti <vtix> address <addr>	Added	VTI
interfaces vti <vtix> description <descr>	Added	VTI
interfaces vti <vtix> disable	Added	VTI
interfaces vti <vtix> mtu <mtu>	Added	VTI
vpn ipsec site-to-site peer <peer> vti bind <vtix>	Added	VTI
vpn ipsec site-to-site peer <peer> vti esp-group <name>	Added	VTI
protocols bgp <asn> maximum-paths ebgp <max-paths>	Added	BGP Multi-path support
protocols bgp <asn> maximum-paths ibgp	Added	BGP Multi-path support

Configuration Mode Parameters	Type of Change	Reason / Comment
<max-paths>		
policy route <name> …	Added	Policy based routing (see the Policy Based Routing guide for a complete list of commands)
policy ipv6-route <name> …	Added	Policy based routing (see the Policy Based Routing guide for a complete list of commands)
protocols static table <table> …	Added	Policy based routing (see the Basic Routing guide for a complete list of commands)
interface <interface-type> <interface> policy route <policy route name>	Added	Policy based routing
interface <interface-type> <interface> policy ipv6-route <policy route name>	Added	Policy based routing
traffic-policy priority-queue <policy-name> …	Added	QoS priority queue (see the QoS guide for a complete list of commands)
vpn ipsec site-to-site peer <peer> …	Modified	IPsec for IPv6 – now accepts IPv6 addresses (see the VPN guide for a complete list of commands)
vpn ipsec site-to-site peer <peer> local-ip changed to: vpn ipsec site-to-site peer <peer> local-address	Changed	VPN changes
vpn ipsec site-to-site peer <peer> tunnel <tunnel> local subnet changed to: vpn ipsec site-to-site peer <peer> tunnel <tunnel> local prefix	Changed	VPN changes
vpn ipsec site-to-site peer <peer> tunnel <tunnel> remote subnet changed to: vpn ipsec site-to-site peer <peer> tunnel <tunnel> remote prefix	Changed	VPN changes

Operational Mode Commands	Type of Change	Reason / Comment
show interfaces vti	Added	VTI
show interfaces vti detail	Added	VTI
show interfaces vti <vtix> brief	Added	VTI
show vrrp	Modified	VRRP operational

Operational Mode Commands	Type of Change	Reason / Comment
		command changes
show vrrp summary	Removed	VRRP operational command changes
show ip route table <table>	Added	Policy based routing
reset vpn ipsec-peer <peer>	Modified	IPsec for IPv6 – now accepts IPv6 addresses
show vpn debug	Modified	IPsec for IPv6 – now accepts IPv6 addresses
show vpn ike sa	Modified	IPsec for IPv6 – now accepts IPv6 addresses
show vpn ipsec sa	Modified	IPsec for IPv6 – now accepts IPv6 addresses

Resolved Issues

The following issues have been resolved in this release.

Bug ID	Severity	Description
BGP		
3651	minor	“no debug bgp” does not disable BGP debugging as indicated
CLI		
7099	trivial	“compgen -\: invalid option” message
7615	major	inodes not getting freed after load/discard
7647	minor	Command complete incorrect when deleting single value on interfaces
8178	minor	Script error setting interfaces in current build
8256	minor	‘… address-group <> address 0.0.0.0’ causing ipset internal error
8257	minor	‘… network-group <> network 0.0.0.0/0’ causing ipset internal error
Configuration Synchronization		
8088	minor	Change ‘show config-sync status’ “last sync status” “good” and “bad” to succeeded and failed
Connection Tracking		
7861	minor	show conntrack table not resolving all known protocols
7998	minor	rename custom timeout chain and insert it after VRRP chain when initializing
8078	major	Kernel Panic – “BUG: unable to handle kernel paging request at 00100100” … “flush_expectations+0x68/0x88 [nf_conntrack_sip]”
8338	major	system conntrack timeout custom, internal errors when multiple source ports and single destination port
8392	major	FTP NAT ALG fails to modify FTP passive response header following a conntrack-sync failover of preexisting FTP connections when the FTP server is behind NAT
Connection Tracking Synchronization		
5874	major	upgrade conntrack-tools and libnetfilter_conntrack packages used by conntrack-sync feature
6843	major	changing conntrack table size when conntrack sync is enabled causes VRRP or clustering to reload disruptively
8243	major	conntrack-sync flushes the entire conntrack table on the new backup system during a state transition
8383	major	Expect table synchronization fails when NAT is used on the Firewall
DHCP		
8293	major	Cannot use the double quote (“) character in a value string
8367	major	CVE-2012-3955: Reducing the expiration time for an Ipv6 lease may cause the server to crash

Bug ID	Severity	Description
Documentation		
7329	minor	Revise Image-based upgrade documentation to include process for supported customers
7457	trivial	Quickstart guide documents installation onto ESX/ESXi 3
7588	trivial	3.0 kernel version number confuses some 3rd party software
7671	minor	Wrong description for “firewall source-validation <state>” at Ipv4 Firewall Commands
7747	trivial	Missing command "interfaces bridge <brx> mac"
8110	minor	add the tunnel interface to the bridge group
8226	minor	Missing documentation for "monitor interfaces vrrp <if> flow"
8239	trivial	RFC3330 is obsoleted by RFC5735
8251	minor	Missing "restart dhcp" command documentation
8263	minor	"firewall name ALLOW_ESTABLISHED" in Quick Start guide is confusing
8324	major	Remove P2P firewall from docs
8335	major	Systems running 64bit virt image of oxnard or older releases should use add system image to upgrade
Entitlement		
7604	major	Sys-id hash collision with VSEDEMO entitlement on bare-metal install
Firewall		
3167	minor	iptables does not match firewall configuration when destination has single port and source has multiple ports
8200	minor	shim6 shouldn't be allowed for "firewall name <> rule <> protocol <>"
8330	major	firewall rule number info isn't provided in the commit failure message
Installer		
7624	minor	perlcritic warnings from vyatta-boot-image
7625	minor	perlcritic warnings from strip-migration-comments
Interfaces		
6967	minor	Interface failure results in 'unrecoverable' configuration
7191	major	Config out of sync with system state when interface address and invalid firewall name assigned in same commit
7976	minor	Local-ip node of tunnels give false warning of missing address
8285	minor	Error setting MTU on bond device VIFs
IPS		
7957	major	Deprecate Snort IPS (content-inspection) functionality
Kernel		
1656	minor	Release a fully-supported 64-bit Vyatta (VSE) build

Bug ID	Severity	Description
Logging		
3921	minor	"show system boot-messages all" displays binary data
7807	critical	Logs can exhaust available disk space causing critical failure of system services
Netflow		
7443	major	netflow daemon dies if it can't contact the server at commit time
OSPFv3		
6412	major	[Quagga] import-list and export-list settings have no effect
7039	major	[Quagga] OSPFv3 process crashes on filter-list setup
Platform		
7202	major	xenserver guest PV boot failed on Xenserver 5.5
7398	major	Deactivating or modifying a network interface crashes xenserver guest
7491	minor	"This system is open-source software" in the welcome message after login is done
7841	major	amd64 xenserver PV guest doesn't boot
PPPoE		
6931	minor	Significant latency added by running PPPoE in user-mode
QoS		
7158	major	traffic-policy limiter with ether source match functions in 6.1 but not in 6.2
8017	major	Qos policy not working when on a Multilink PPP vif interface
RAID		
8210	minor	'add raid <> member <>' returns internal error when <> is 'abc'
SNMP		
8080	major	incorrect agent index can crash SNMP (CVE-2012-2141)
System		
3241	minor	Password reset does not work if the config file fails to load completely
5511	major	telnet process cannot recover via cli after failure
5792	trivial	Show system image commands output on livecd
6576	major	Drop support for SSH v1
6886	minor	perl critic warnings in image scripts
7656	major	Changing 'system domain-name' does not modify /etc/hosts as needed
7657	major	FQDN not properly set using 'system host-name' and 'system domain-name'
7815	minor	Add dialog package
7964	major	Change 'add system image' default value for configuration directory copy option when not enough disk space exists

Bug ID	Severity	Description
7985	major	"rename system image" renames multiple images when old image name is a substring of >1 installed image name
8274	minor	Invalid commands in "show tech-support" output
8287	minor	Commits of user deletions should succeed if the user does not exist
8290	blocker	Don't allow password to be default "vyatta"
8380	minor	error: "sudo: unable to resolve host [hostname]" when commiting new system host-name
Virtualization		
8245	major	virt iso (32 bit) and xen template fails to boot on XenServer and Xen domU
VPN		
6893	trivial	perl critic warnings in VPN
8402	major	Vyatta initiates main mode despite configured as responder.
VRRP		
8075	minor	Remove superfluous addr type column from 'show vrrp summary' output
8107	major	VRRP with 400+ vlans with VRRP instances Goes into endless loop
8125	minor	Errors seen when running the opmode command 'sh vrrp ' when no vrrp is configured
8146	minor	'show vrrp' displays spurious output following an interface deletion
8177	minor	Use of uninitialized value $vip in printf at /opt/vyatta/bin/sudo-users/vyatta-show-vrrp.pl line 199.
8271	minor	Vestigial hooks and chains in netfilter raw table - VYATTA_VRRP_FILTER, VYATTA_VRRP_OUTPUT_FILTER
8356	major	ARP requests from VRRP IP address should be sourced from the VRRP MAC in RFC 3768 compatibility mode
WebGUI		
1570	minor	GUI: Certificate does not match configuration
4091	minor	Cannot set time zone
7509	major	"set service https" enables http in addition to https
7510	major	"set service https listen-address" does not affect http listen-address
7636	minor	Web interface broken when adding complex snmp community name
7773	minor	ENH: using the tab key after password input does not direct the user to the login button
7796	minor	Description sorting under the interface tab is not done correctly
7843	major	a gui session doesn't get timed out soon enough when a system goes down.
7879	minor	ENH: the more info boxes should automatically adjust in vertical spaces

Bug ID	Severity	Description
7925	minor	no loading page when the user is redirected to the statistics page from the interfaces subsection on the dashboard
7978	minor	navigating to the statistics page from the dashboard for an interface that does not have traffic flow shows no y -axis
8025	minor	WebGUI: remote-access VPN more info call-out unable to parse user names that are longer than 10 characters
8027	minor	WebGUI: Configuration redirect from the interfaces sub-section on the dashboard does not complete for remote-access VPN interfaces
8035	minor	WebGUI: config-management more info call-out should sort on time column
8045	minor	WebGUI: DNS Servers more info call-out values are not properly sorted
8046	minor	WebGUI: System Time display on dashboard contains hyphens making it inconsistent with other locations that display time/date output
8048	minor	WebGUI: zones more info call-out should display non-zone interfaces detail
8050	minor	WebGUI: Statistics graph displays negative values when sending traffic over an OpenVPN interface that is down
8094	major	Disable SSLv2 encryption in HTTPS service
8138	major	Hide restart https from the gui under the operation tab
Wireless		
6556	major	Problems with wireless when using radius server for WPA (hostapd)

Known Issues

Bug ID	Description
AMI	
7450	"Failed to read ..." errors can display on the console when an AMI instance boots. Recommended action: None. This issue is display-only.
BGP	
5822	The "neighbor <peer-group-name> ebgp-multihop 255" configuration entry appears in the routing engine after committing “delete peer-group <peer-group-name> remote-as <>". This issue only occurs when the peer-group remote-as is the same as the local one, i.e., the peer-group is iBGP. Recommended action: Remove the peer group entirely; alternatively, issue the following command vtysh –c 'conf t' -c 'router bgp *local-asn*' -c 'no neighbor *peer-group-name* ebgp-multihop'
6042	The BGP "confederation peers asn" option cannot be used after the peer's ASN configuration has already been committed. Recommended action: None.

CLI	
2777	Stray quote confuses CLI. Accidentally typing a single quote puts the CLI into a mode where it expects additional input, as in the following example: root@charon# set interfaces ethernet eth' [edit] root@charon# commit > > > This occurs in both operational and configuration mode. Recommended action: Avoid typing stray single quotes when entering commands. Note: This is currently designed behavior. For more information about using the Vyatta CLI, please see the "Using the CLI" chapter of the *Vyatta Basic System Reference Guide*.
5065	A commit error is generated if a firewall "name" configuration is deleted at the same time as deleting the assignment of the firewall "name" to an interface. Recommended action: Delete the assignment and commit the change, then delete the "name" configuration and commit the change.
6902	The Vyatta CLI does not properly support double quotes in configuration values. Recommended action: Avoid using the double quote character (") in configuraiton strings.
Clustering	
3105	If two clustered routers reboot when the master router's monitored interface is down, the master still becomes active. This issue occurs only when both routers are booting and the master's monitored interface is disabled in configuration. After the routers come up, master negotiates to active even though its interface is disabled. If the interface is enabled, traffic flows normally. If the interface is disabled again, the routers fail over as expected. This issue does not occur if fewer than 15 services are entered in the cluster. This issue does not occur if the two routers are rebooted with a gap of 30 seconds or greater. Recommended action: Reboot the primary router, or delete the cluster configuration on the primary router and reload the configuration.
DHCP	
2657	Lease expiration is not displayed in local time; it is displayed in GMT timezone only irrespective of the system's configured timezone. Recommended action: None.
Firewall	
6965	The "show firewall" command returns incorrect information for 'packets' and 'bytes' after some million packets are traversed. Recommended action: None.
7733	A connection tracking table larger than 1 MB causes a kernel memory allocation failure, leading to a system crash. The firewall allows the user to set the conntrack table size larger than the available kernel memory can support. Recommended action: Avoid setting the size of the conntrack table larger than 1 MB.
Installer	
6135	An error occurs when the install-system command is executed at the point where the default root partition size is chosen and the install fails. Recommended action: If this problem occurs, manually select a partition size slightly smaller than the size reported by the drive. Install should subsequently be successful.
8306	While installing the system is reporting that it detects RAID groups and two drives drives on a system booted from LiveCD. This appears to be a driver problem.

	Recommended action: None.
Interfaces	
6714	A vif interface cannot be deleted if it belongs to a bridge. Recommended action: To avoid this problem, delete the vif's bridge configuration before deleting the vif itself.
Kernel	
5295	Connection tracking helper modules cannot re-assemble application layer PDUs residing in two or more TCP segments. This is typically only a problem when an application layer PDU is larger than 1500 bytes. The result of this issue is that the application can fail. Recommended action: None.
8322	Emulated network interface (driver tulip) shows link down, fails to come up in Hyper-V An emulated network adapter using the "Tulip" driver fails when booted from LiveCD. The link is not detected and the link status shows as "down." Recommended action: To avoid this issue, use a synthetic network adapter. If this issue occurs, clear the link by shutting down the link administratively and bringing it up again.
Load Balancing	
7503	The WAN load balancing feature is changing the source interface and address during outbound session from the inside. As a result, HTTPS sites (such as webmail and banking sites) are requiring the user to reauthenticate during the session. Recommended action: To prevent this issue, create a separate WAN load balancing rule that exclusively binds HTTPS traffic to a particular outbound interface. If you do this, however, the HTTPS traffic does not receive the bandwidth aggregation benefits of load balancing.
Netflow	
8424	If an interface is added after the Netflow server is defined, the system displays a "flow-accounting is not running" message. Recommended action: If this issue occurs, restore normal function by saving configuation, then deleting flow accounting configuration, then loading and committing the saved configuration.
OSPF	
3004	Deleting an OSPF area may fail if the network entry is not a connected network and virtual links are in use. The configuration commit fails with an "Area does not exist" error message. Recommended action: Remove virtual links included in an OSPF area configuration prior to deleting the OSPF area.
3348	OSPF process dies if the router ID value is modified while OSPF routers are converging. This issue may also occur after convergence if the OSPF router ID is changed twice within a short interval. Recommended action: If the OSPF router ID must be changed, it must be changed after OSPF routers have finished converging, when OSPF adjacencies are stable and OSPF routes in the RIB are synced with OSPF LSAs.
6762	A "delete protocols ospf" operation fails if the "passive-interface-exclude" option has been configured. Recommended action: Delete the "passive-interface-exclude" configuration setting before deleting OSPF configuration.
Platform	
7494	A kernel panic occurred for a XenServer guest during a boot in PV mode. The issue occurred using the 3.0.4 virt kernel prepared using the "install-image" command. Recommended action: To avoid this problem, use the "add system image" or "upgrade system image" commands to install or upgrade your system.
Policy	
6166	Configuration commit fails when a route-map is deleted using the "comm-list" option. Recommended action: To avoid this problem, do not attempt to delete using the "comm-list" option

	if it is already set. Alternatively, use the “set community” command with values that exclude the community to be deleted.
8340	The output of the “show policy” command includes unnecessary and irrelevant information. Recommended action: None.
8341	The output of the “show policy” command does notinclude policy table information. Recommended action: None.
8342	When a policy rule set was modified to refer to an unused table and configuration is committed, an internal error occurs. Recommended action: None.
8343	If a routing policy rule is deleted and the deletion committed, then the rule is removed from interface configuration and the change configured, the system fails the deletion, reporting an error. Recommended action: None.
8354	In routing policy rules, the system should prevent configuring “action drop” and “set” options at the same time. Recommended action: None.
8364	If a routing policy rule is already applied to an interface, then if the rule is modified to include the “set tcp-mss” option, the system fails to commit the configuration change. If the policy route <> is already set under an interface, then internal error when it’s modified/committed with set tcp-mss - Recommended action: None.
RIB	
7952	If a static route is configured to exit through an interface and that interface is subsequently configured with an IP address, the static route is lost from the RIB. Recommended action: None.
SNMP	
5442	64-bit SNMP traffic counters do not work for all ethernet interfaces Recommended action: Use SNMP OIDs for 32-bit counters instead of 64-bit for unsupported interfaces.
Static Routes	
5905	If the distance for a static IPv6 route is updated or deleted, the change is not recorded in the routing engine. Recommended action: Delete the route, then set it again with the new distance.
System	
6952	The system reports the following message if it boots immediately prior to receiving a login prompt: ata2: failed to resume link (SControl 0) Recommended action: None. This issue is display-only.

8410	If a configuration file contains user accounts with a password of "vyatta", the system's default password prevention mechanism forces the user to change the password and the system then performs an automatic save of the config.bootfile. This automatic save occurs before the user can access the system. If subsequently this same configuration fails to load completely due to a syntax validation check, any section of the configuration that failed to load is removed and replaced by the running configurationduring the password auto-save process on login.
Virtualization	
8333	Microsoft's System Center Virtual Machine Manager 2008 displays a warning when a guest VM is created , using either an ISO or a virtual hard disk. The "VM create" job completes with the following warning message: Virtual Machine Manager cannot locate the boot or system volume on virtual machine. The resulting virtual machine might not start or operate properly. However, the virtual machine starts and operates correctly. Note that if the Hyper-V Manager is used to create the guest VM, no warning is displayed. Recommended action: This warning has no operational effect and can be safely ignored.
VPN	
8359	Deletion and adding vti deletes vti interface in show interfaces output though vti configuration exists Recommended action: None.
8420	If an IPv6 site-to-sitepeer address is configured with all zeros (the "wildcard" address), the system converts the address the IPv4 version, 0.0.0.0. As a result, the tunnel not able to attain an ISAKMP SA established state. Recommended action: None.
8430	If the IPsec process starts and assigns a default route before the DHCP server has assigned the IP address to the DHCP client, the tunnel fails to come up. Recommended action: If this occurs, restart IPsec process; the tunnel will be brought up correctly.
VRRP	
7703	The kernel only allows one of bridging, bonding, VRRP, and pseudo-Ethernet to be selected, but Vyatta templates do not enforce this restriction for VRRP and pseudo-Ethernet. Additional checks should be implemented in the templates to enforce this restriction for devices using bonding or bridging. Recommended action: None.
Web GUI	
7354	When Safari is used as the web browser, duplicate requests are sent to the server. Recommended action: Use supported web browsers: Firefox, Chrome, and Internet Explorer.
Web Proxy	
4952	If the web proxy feature is configured together with clustering, both configurations may be lost. Recommended action: None.