

VYATTA, INC. | **Release Notes**

Vyatta Release 6.0 Beta

February 2010

Document Part No. A0-0095-10-0020



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

Contents

These release notes document changes in Release 6.0 Beta.

- Security
- New in This Release
- Behavior Changes
- Documentation Changes
- Upgrade Notes
- Resolved Issues
- Known Issues

Security

There are no security announcements in this release.

New in This Release

In this release, Vyatta delivers three distinct product offerings, as follows:



- **Vyatta Core.** The Vyatta Core (VC) is the core set of features and functionality available in the open-source, unsupported version of the Vyatta networking, security, and services platform. The Vyatta Core is freely distributed to the community. The Vyatta Core is represented using the icon at left.



- **Vyatta Subscription Edition.** The Vyatta Subscription Edition (SE) is Vyatta's premier product and represents expanded feature sets and packaged services that are available only to Vyatta subscribers. The Vyatta SE includes all of the features distributed in the Vyatta Core plus proprietary Vyatta features, as well as selected third-party features and functionality. The Vyatta SE is supported by the Vyatta Technical Assistance Center and provides access to all bug fixes, security patches, and continual product enhancements. Vyatta SE is available as software, virtual machines, and Vyatta hardware appliances through Vyatta sales, Vyatta's web store, and authorized Vyatta partners. The Vyatta SE is represented using the icon to the left. This icon is also used to identify Vyatta SE features in Vyatta product documentation.



- **Vyatta Plus.** Vyatta Plus features are add-on services or enhancements to the Vyatta Subscription Edition, available for an additional service fee. Vyatta Plus features are available only to Vyatta Subscription Edition customers. Vyatta Plus is represented using the icon at left. This icon is also used to identify Vyatta Plus features in Vyatta product documentation.

Release 6.0 Beta of the Vyatta system includes features for the Vyatta Core as well as features for the Vyatta SE and Vyatta Plus.



The following new features are available for the Vyatta Core:

- **Wireless interface support.** The Vyatta Core now supports IEEE 802.11 wireless LAN (WLAN) support (commonly referred to as Wi-Fi) for compatible hardware. The Vyatta system supports both Wireless Access Point and Station support. For information about wireless interface support, see the *LAN Interfaces Reference Guide*.
- **Flow Accounting.** This release provides the ability to locally display information about network traffic, as well as the ability to export this information to Netflow- or sFlow-compatible collection servers. For information about flow accounting support, see the new *Network Accounting Reference Guide*.
- **IPsec VPN enhancements.** The IPsec site-to-site VPN functionality has been extended and support implemented for many enhancements requested by the community and customer base.
- **Enhancements to WAN load balancing.** WAN load balancing now includes the ability to set a rate limit on outgoing interfaces. Traffic exceeding the configured threshold uses an alternate interface. Interface health tests have been expanded to include a time-to-live limit test and the ability to specify multiple test targets for an interface. For information about WAN load balancing, see the *Availability Reference Guide*.
- **SSH enhancements.** In addition to standard SSH password authentication, the Vyatta Core now supports public key authentication for SSH. The administrator can disable password in the CLI, so that only users with shared credentials can log on over SSH. This extra security helps prevent brute force password attacks on servers running SSH. Public keys are loaded onto the system by the administrator and stored encrypted as part of system configuration. Also, when installing the system using the **install-system** command, the Vyatta Core now provides the option of preserving old SSH host keys, eliminating SSH-related warning messages after installation. For information about SSH configuration, see the *IP Services Reference Guide*.
- **SNMP enhancements.** The Vyatta Core now allows you to configure a source address or interface for SNMP traps. This feature allows the administrator to limit traps to a known set of source IP addresses. Trap targets can now each be configured with a separate community string and port. The delay between Ethernet link-state changes and the generation of SNMP linkUp and linkDown traps has been significantly reduced and the trap now includes output from the ifIndex, ifDescr, ifType, ifAdminStatus, and ifOperStatus objects of the IF-MIB. In addition, the sysDesc and sysObjectID objects are now populated according to the version of the system installed. For information on SNMP support, see the *Basic System Reference Guide*.
- **DHCP server options.** The Vyatta Core now provides the ability to configure DHCP server options not specifically available through dedicated commands. Options are configured as text strings, which allow custom options to be entered (provided the text conforms to standard DHCP option syntax). Options can be specified at four different levels of scope: global, shared network, subnet, and

static mapping. For information about DHCP support, see the *IP Services Reference Guide*.

- **Installation from system image.** This release provides the ability to install and upgrade from a single binary system image. Multiple system images can be obtained from the Vyatta web site and stored on your system, allowing for easy upgrades and downgrades using the new **install-image** command. For information on installing and upgrading from a system image, see the *Installing and Upgrading Reference Guide*.
- **IPv6 SLAAC.** The Vyatta Core now supports the router side of the IPv6 stateless address auto-configuration (SLAAC) protocol, as defined in RFC 4862, and Router Advertisements (RAs). Please note that IPv6 features remain experimental* at this time. For information about IPv6 SLAAC, please see the *Guide to IPv6 Support*.
- **IPv6 routing policies.** Routing policy support has been extended to IPv6. Please note that IPv6 features remain experimental* at this time. For information about IPv6 routing policies, please see the *Routing Policies Reference Guide*.

* Experimental Features: Please note that Vyatta software is in an ongoing development cycle, and from time to time experimental features are included in releases. Features noted as experimental have not undergone Vyatta's complete QA testing cycle and as such have limited support.



The following new features are available for the Vyatta Subscription Edition:

- **TACACS+.** The Vyatta Subscription Edition now supports the use of a Terminal Access Control Access-Control System Plus (TACACS+) central server for authenticating users. TACACS+ can be used with Vyatta login credentials on the local system or without a local user account. For information on TACACS+ support, see the *Basic System Reference Guide*.
- **Integration with OpenAccess VPN server.** The Vyatta Subscription Edition now supports client-side remote access for accessing configuration information from an OpenVPN Access Server. The OpenVPN Access Server authenticates remote client access requests (either locally or by means of an authentication server) and provides OpenVPN tunnel configuration information to the requesting client. The client can then establish an OpenVPN tunnel with an OpenVPN server with minimal configuration on the client side. For information about OpenVPN support, see the *VPN Reference Guide*.



The following new service is offered through Vyatta Plus:

- **Vyattaguard enhanced web filtering.** In addition to the community-based URL filtering in Vyatta Core, Vyatta now offers Vyattaguard enhanced web filtering as an add-on service to the Vyatta Subscription Edition. Vyattaguard advanced web filtering helps organizations implement Internet security policies and promote workplace productivity by blocking access to unwanted Internet sites and enforcing Internet use policies. Vyattaguard web filtering adds enhanced protection and policy enforcement using a commercial database containing 100 million+ categorized URLs as compared to the community-compiled database available in the Vyatta Core web filtering feature. In addition, the Vyattaguard can use the network to classify URLs not found in the local database or not

found on small appliances with no local database. Support for existing web filtering in Vyatta Core remains unchanged. For information about Vyattaguard web filtering, see the "URL Filtering" chapter of the *Security Reference Guide*.

Behavior Changes

- **Serial support.** Serial communications card and protocol support is now a Vyatta Subscription Edition feature. Support for serial features is no longer available in the Vyatta Core.
- **IPsec VPN aggressive mode.** In this release, support for aggressive mode in IKE Phase 1 key exchange has been removed from the IPsec VPN implementation (that is, the `vpn ipsec ike-group group-name aggressive-mode` command has been obsoleted). After upgrade to this release, only main mode will be supported. This change affects interoperability with a Vyatta VPN peer running a prior release and configured to use aggressive mode for IKE Phase 1 key exchange. After upgrade, the peer must be configured to use main mode for key exchange.
- **IPsec VPN logging.** Starting with this release, logging facility and logging level can no longer be set for IPsec VPN (that is, the `vpn ipsec logging facility` and `vpn ipsec logging level` commands have been obsoleted). After upgrade to this release, the IKEv1 daemon logs messages with `facility=authpriv`. To record IKEv1 messages, ensure that syslog is configured to log messages from processes using the `authpriv` facility. The `vpn ipsec logging log-modes` command continues to be supported.
- **SSH and Telnet.** The syntax of the SSH and Telnet commands `set service ssh allow-root` and `set service telnet allow-root` have changed. These commands no longer require (or accept) a value of `true`. To enable root SSH or Telnet access, simply specify `set service ssh allow-root` and `set service telnet allow-root`, respectively. SSH and Telnet configurations in supported upgrade paths using the old syntax are automatically migrated during upgrade.
- **SNMP.** SNMP configuration has been moved from the `protocols snmp` configuration node to a new `service snmp` configuration node. SNMP configurations in supported upgrade paths are automatically migrated to the new syntax during upgrade.
- **WAN load balancing.** The `ping` and `resp-time` options have been moved from being subnodes of the `interface-health` configuration node to being subnodes of the `test` configuration node. WAN load balancing configurations in supported upgrade paths are automatically migrated to the new syntax during upgrade.

Documentation Changes

- **New:** *Network Accounting Reference Guide*. To support the new Flow Accounting feature, a new *Network Account Reference Guide* has been prepared.
- **New:** *Guide to Vyatta Software Licensing*. To support access to subscription-only features in the Vyatta SE and Vyatta Plus, Vyatta has implemented a licensing and entitlement infrastructure. This infrastructure is described in the new *Guide to Vyatta Software Licensing*.
- **Consolidated:** Installation and upgrade information. Information on installing the Vyatta system to VMware and XenServer platforms has been consolidated into the *Installation and Upgrade Guide*.

Upgrade Notes

For detailed information about upgrading Vyatta software to this release, please see the *Vyatta System Installation and Upgrade Guide*.

Resolved Issues

Bug ID	Severity	Component	Description
BGP			
4376	major	BGP	CLI Error on creating Policy Route-Map
4467	major	BGP	System clock fluctuations appear to adversely affect routing protocol timers
4964	unassigned	BGP	BGP Community tab completion of well known communities
4984	minor	BGP	Configuring an IP of a local interface as a bgp neighbor results in an out of sync condition between the vyatta config and the bgpd config
5035	unassigned	BGP	bgpd is crashed after multiple bgp neighbor route-server-client are deleted and committed
5119	unassigned	BGP	bgp daemon crashes when configuring allowas-in and shutdown after peer is established
5155	critical	BGP	bgp peer resets when adding ip address to another interface
5201	unassigned	BGP	vyatta-bgpd can't accept vty socket - Too many open files
CLI			
4359	minor	CLI	vyatta-save-config.pl intermittently parses entire filesystem into enormous config.boot.\$PID files when called by cron
4757	enhancement	CLI	wrong spelling
5028	unassigned	CLI	BGP password containing special characters not correctly passed to quagga
DHCP			
3049	enhancement	DHCP	Add custom option support to DHCP configuration within CLI

4674	minor	DHCP	Error configuring DHCP relay
4749	enhancement	DHCP	add ability to disable a static-mapping under dhcp-server
4750	enhancement	DHCP	add ability to disable a shared-network under dhcp-server
4754	minor	DHCP	DHCP client sends wrong hostname
5171	unassigned	DHCP	dhcp client broken in kenwood
Firewall			
3625	enhancement	Firewall	Firewall protocol option should have a selection for TCP and UDP
3757	unassigned	Firewall	"Firewall config error: Cannot delete ..." after a config with a different firewall set under same interface is loaded
4156	minor	Firewall	FW: Firewall names should not accept the space as a valid character.
4495	minor	Firewall	Invalid interfaces are accepted in zone policy
4998	unassigned	Firewall	Firewall ruleset being used by IDS is reported as not applied
5227	unassigned	Firewall	firewall group config can get out of sync with ipset
5248	major	Firewall	Firewall config and show commands hang when showing and committing address groups
5326	major	Firewall	"set firewall group address-group <NAME> address <StartIP>-<EndIP>" fails on commit when last octet of EndIP is 255 and any address exists in the group matching the first three octets
GUI			
1223	major	GUI	System does not notify user of reboot
1234	minor	GUI	GUI - if http service is deleted no indication is provided to active GUI sessions
2765	major	GUI	Add Vyatta logos with registered trademark symbol to GUI
3899	unassigned	GUI	Wrong license on GUI
4087	minor	GUI	Table sort order
4141	major	GUI	GUI - logs user out by mistake
4143	trivial	GUI	Split header line in operational commands
4145	minor	GUI	"Stop" button may be ineffective
4154	major	GUI	GUI does not display meaningful error messages on first commit failure
4155	minor	GUI	GUI: Red error indicators disappear after correcting first missing value for NAT rule
4177	major	GUI	webgui load command doesn't work with remote files
4185	enhancement	GUI	Display a warning message with an option to set or discard when leaving a page with unset changes
4186	enhancement	GUI	Generate a warning message when the discard button is pressed
4224	minor	GUI	Need to allow the option to configure NAT interface for eth+
4231	minor	GUI	Web GUI is sorting NAT rules wrong
4253	major	GUI	GUI: Deleting a single address value on a multinetted interface deletes all address values
4415	minor	GUI	Previous element displayed at top of configuration window
4635	minor	GUI	GUI process logs internal errors
4853	minor	GUI	Web GUI can fill disk with output chunks in /opt/vyatta/tmp/webgui

IDS			
4847	unassigned	IDS	snort local.rules gets overwritten on rules update
5099	unassigned	IDS	Content Inspection commit fails due to timeout
Interface			
4419	enhancement	Interface	Add ability to configure ethernet flow-control and checksum-offload
4994	minor	Interface	Committing speed and duplex changes are considered successful while not supported by the interface
5014	trivial	Interface	show interfaces - vif descriptions shown as VAR(@)
5031	enhancement	Interface	Add the option to set the arp_ignore value via the CLI
5143	trivial	Interface	Incorrect auto IRQ affinity assignment when NIC has 10 or more queues
5223	minor	Interface	Serial MTU and MRU settings removed between Isla Vista and Jenner without config migration
5312	major	Interface	IPv6 Neighbor discovery fails to work on bonded interfaces following a reboot
IPv6			
3696	unassigned	IPv6	ipv6 address lost when bringing the interface down
4892	critical	IPv6	Add parameter to disable IPv6 features
Kernel			
4428	minor	Kernel	Disable copybreak in NIC drivers that support it
Load Balancing			
3704	major	Load balancing	Don't flush mangle prerouting table on ping target failure
3953	enhancement	Load balancing	Allow multiple ping targets for wan-load-balancing interface health checks
4072	unassigned	Load balancing	Add "Load-Balancing" Rule Description Option
4083	minor	Load balancing	WLB show commands display configured interfaces in the reverse order
4248	enhancement	Load balancing	Add a 'clear wan-load-balancing' command to the Vyatta CLI
4587	minor	Load balancing	WLB status indicates active if previously configured
4649	enhancement	Load balancing	Add a 'clear wan-load-balancing process' command to the Vyatta CLI
4762	unassigned	Load balancing	new connections to the inbound-interface can't be established after load-balance wan is set/committed
Logging			
3528	enhancement	Logging	Netflow support
NAT			
1445	enhancement	NAT	Service nat protocol option should have a selection for TCP and UDP w/o including ICMP
4115	minor	NAT	"clear nat translations" does not clear nat translations
4751	enhancement	NAT	add ability to disable a NAT rule
4780	unassigned	NAT	DNAT rule to translate just port fails
OSPF			

4014	minor	OSPF	Can't configure OSPF passive on dynamic interface
4161	enhancement	OSPF	Bad config handling of "protocols ospf passive-interface"
4421	major	OSPF	Removing OSPF redistribution is excessively slow
5036	major	OSPF	Unable to configure more than one interface per area in OSPFv3
Policy			
3697	minor	Policy	Policy set metric value is not removed from routing engine config when deleted from CLI
5015	major	Policy	Route maps terms that contain reference to VIF interfaces fail to load on boot
5060	unassigned	Policy	error adding bgp policy to ipv6 peer
PPP			
5288	major	PPP	Multilink PPP drops last fragment in sequence in some cases
PPPoE			
4679	minor	PPPoE	Administrative user cannot clear connection
QoS			
4450	minor	QoS	random-detect (and some traffic-shaper) policies confuse show queueing
4526	minor	QoS	traffic-shaper inaccurate at higher speeds
4920	unassigned	QoS	"... qos-policy out <>" is out of sync with "show queueing" result
4978	enhancement	QoS	qos for tagged traffic
5005	major	QoS	Unable to apply QoS policy to PPPoE interface
5109	minor	QoS	No option exists for pppoe under 'show queueing'
5138	unassigned	QoS	Numbering QoS classes greater than 9 is not translated correctly
5245	minor	QoS	show interfaces ethernet ethx vif xx
Serial			
4638	minor	Serial	Administrative user cannot run loopback test
4639	minor	Serial	Loopback up/down commands do not tab complete
5216	critical	Serial	Sangoma card does not come up during a reboot or softboot
5224	minor	Serial	qos-policy settings relocated between Isla Vista and Jenner without migration
SNMP			
212	enhancement	SNMP	Change Request: SNMP configuration
468	enhancement	SNMP	Feature Request: SNMP Trap Source
2552	trivial	SNMP	SNMP: snmpd daemon using deprecated sysctl (net.ipv6.neigh.lo.retrans_time)
3533	unassigned	SNMP	snmpwalk/snmpbulkwalk host fail when there are 100 Ethernet vif sub-interfaces
3755	enhancement	SNMP	ENH: SNMP: Allow setting default snmp trap community
3756	enhancement	SNMP	ENH: SNMP: Allow setting multiple SNMP trap targets with varying communities and port numbers
3806	major	SNMP	SNMP: Excessive delay between link state changes and linkUp/linkDown trap generation

3811	major	SNMP	SNMP: Trap payload does not include appropriate OIDs
3869	major	SNMP	SNMP: sysDescr and sysObjectID need to be dynamically populated
4471	minor	SNMP	snmpd keeps shadow records of ppp interfaces
4499	trivial	SNMP	config not removed from snmpd.conf after "delete protocols snmp" then "commit"
4523	minor	SNMP	Incorrect speed reported for down interfaces
4524	unassigned	SNMP	SNMP interface speed report broken for 10Gb and above
Static			
4871	unassigned	Static	add ability to disable static routes
5101	unassigned	Static	arp command for static needs to be run under sudo
System			
3368	trivial	System	SYSTEM: Kernel panic when running shutdown -h from livedcd.
3546	enhancement	System	Disable pager for root
4081	major	System	SYSTEM: Cannot SSH from a Vyatta to the same Vyatta. (installed system only)
4256	unassigned	System	open-vm-tools does not load in ESXi3.5
4386	trivial	System	Rename /etc/init.d/vyatta-ofr
4604	enhancement	System	Add kernel command line parameter to boot without Vyatta config
4951	minor	System	Don't fail if IPv6 module not loaded
4980	minor	System	full-upgrade fails if /etc/squid3/squid.conf does not exist
5226	trivial	System	Hostname does not allow number as first char
5325	unassigned	System	vyatta-cfg-system fails to upgrade during full-upgrade from VC5 to VC6
5328	major	System	linux-image fails to upgrade during full-upgrade from jenner to kenwood
5334	unassigned	System	services start automatically on boot up after full-upgrade to kenwood
5337	minor	System	update copyright line in vyatta version file to 'Copyright: 2006-2010 Vyatta, Inc.'
5340	unassigned	System	full-upgrade from jenner to kenwood downgrades snort packages before upgrading them
5348	unassigned	System	typo in text of download/install
VPN			
1704	unassigned	VPN	Duplicate ESP SAs are being created with auto=start
1714	major	VPN	Vyatta fails to bring up VPN after remote site SA deletion from Cisco
1822	unassigned	VPN	VPN: NAT Network feature is not working
1832	unassigned	VPN	VPN copy-tos: Disabling copy-tos field doesn't work
1833	unassigned	VPN	VPN: Aggressive mode needs patch from Openswan to work with %any configuration
1842	unassigned	VPN	VPN: Compression feature is not working
2388	minor	VPN	VPN process is restarted when an interface is added or deleted
3011	minor	VPN	Remote VPN configuration issues site-to-site warning

3526	enhancement	VPN	Add option to limit L2TP daemon traffic to IPSec
3745	critical	VPN	After the 11th peer is set and committed, "show vpn ipsec sa" returns "VPN is not running"
3770	unassigned	VPN	vpn pre-shared keys should be obscured in "show configuration"
4017	enhancement	VPN	Add the ability to restart individual IPSec tunnels
4021	minor	VPN	VPN: perl errors with incomplete vpn site-to-site config
4377	minor	VPN	Unable to create IPSec tunnel using PSK and %any for remote peer when remote peer is a non-Openswan device
4725	major	VPN	IPsec Site to Site and L2TP IPsec do not play well together
4872	unassigned	VPN	add support for disabling L2TP remote-access user
5052	unassigned	VPN	`clear vpn remote-access user <>` command does not work when radius assigns client IPs
VRRP			
4961	enhancement	VRRP	Enh: Support VRRP on bonding interfaces and vifs thereof
5133	unassigned	VRRP	vrrp transition scripts not working properly when going to backup
Web Proxy			
4038	enhancement	Web proxy	Webproxy: Implement Safe Search Feature for popular search engines
4960	unassigned	Web proxy	url-filter doesn't validate source-group used by rule
5329	unassigned	Web proxy	full-upgrade from VC5 to VC6 stuck while squidguard tries to rebuild database
Wireless			
5188	major	Wireless	error deleting wireless interface

Known Issues

Bug ID	Component	Description
Bridging		
5064	Bridging	<p>If multiple configuration delete operations are performed using the "delete interfaces ethernet <> bridge-group" or "delete interfaces bridge <>" commands, the configuration commit may fail.</p> <p>Recommended action: To avoid this problem, commit each deletion individually.</p>
Load balancing		
5126	Load balancing	<p>DHCP does not work when PPPoE is used together with WAN load balancing failover.</p> <p>Recommended action: None.</p>

OpenVPN		
5207	OpenVPN	<p>The OpenVPN access server client process does not come back up after reboot.</p> <p>Recommended action: Clearing the tunnel using the "clear openvpn vtun <i>tunnel</i>" command restarts the process and restores client-side operation.</p>
OSPF		
5283	OSPF	<p>OSPF IA routes for wireless interfaces are not advertised to neighbors.</p> <p>Recommended action: None.</p>
System		
5362	System	<p>SSH: After deleting public-level SSH keys, the keys remain in the system. The key is removed from the configuration file but not from the underlying key file; therefore, a client with the removed key can still authenticate successfully.</p> <p>Recommended action: Manually removing the .ssh/authorized_keys file deletes all SSH public keys. To do this, issue the command "sudo rm /home/<i>username</i>/.ssh/authorized_keys".</p>
Wireless		
5336	Wireless	<p>By design, multiple SSIDs should be supported on a single physical interface when the interface is configured to use Wireless Access Point (WAP) mode. Currently, multiple SSIDs are supported only on certain hardware/driver combinations.</p> <p>Recommended action: None.</p>