OpenVPN update

Gert Döring

October 27, 2016

RIPE 73, Madrid

OpenVPN 2.4 closing in

- OpenVPN development branches
  - "release/2.3" branch - "stable", no new features, at 2.3.12
  - "git master" - all the more interesting new stuff
  - "master" will become 2.4.0 really soon now
  - 3.x branch - full new code base, C++, client-only, for iOS
- 2.4_alpha2 has been tagged and released two weeks ago
  - 2.4.0 targeting "end of 2016"
- https://github.com/OpenVPN/openvpn/blob/master/Changes.rst

2.4 highlights: Windows

- Windows privilege separation (Vista+)
  - new windows service introduced: “interactive service”
  - OpenVPN GUI and openvpn.exe now run with user privileges
  - ip address config and route setting is done by the interactive service with “system” privileges
  - much smaller attack surface that has to run with elevated privs
- Windows “background service” rewritten to be more robust

2.4 highlights: Crypto

- support AES-GCM crypto modes now
- 2.4 client ⇔ 2.4 server can negotiate data channel cipher
  - `--cipher` was non-negotiable and "the same for all clients"
  - with this, you can upgrade your server and clients one-by-one
- generally fully compatible with older peers (2.1 . . . 2.4)
- TLS cipher defaults have been tightened up
  - this caused issues with certain MikroTik builds - upgrade

2.4 highlights: IPv6

- full dual-stack support
  - 2.3 is more “dual single-stack” (v4-only or v6-only)
  - 2.4 does proper getaddrinfo() try-them-all
  - with that, 2.4 properly works on NAT64/DNS64 networks
- handle overlapping v6-over-v6 gracefully
  - 2.3 would go into loop and explode
  - 2.4 will install v6 host-route to VPN server to avoid overlap

2.4 highlights: roaming

- 2.4 server can assign "peer-id" to 2.3 or 2.4 clients
- when client roams to a new public IP address (NAT state loss, wifi/3G, ...), server will match peer-id with that client's pubkey, and seemlessly roam to new IP
- VPN connection will not need to be re-established
- (UDP only, obviously)

2.4 minor features

- dropped Windows XP support
- added IBM AIX support
- options to tweak per-client options pushed server ⇒ client
  - –pull-filter (ignore certain options sent from server)
  - –push-remove (remove previously set “generic” options)
- LZ4 compression
- tons of bugfixes

2.4.0 code quality

- every single commit pushed to git gets compiled and tested on all architectures supported
  - FreeBSD, NetBSD, OpenBSD, on i386, amd64, sparc64
  - OpenSolaris
  - Linux (umpteen variants)
  - macOS X 10.11 amd64
  - Windows (compile-tested only, no automated testing yet)
- test runs include full-blown VPN tests “connect, transmit data, disconnect, cleanup” on client and server
- so we’re fairly confident the code is as good as 2.3.x

2.4.0 code quality (2)

- *BUT...*
- OpenVPN has WAY too many options
- people use OpenVPN *because* it has all these knobs
- but it makes testing of all possible corner cases impossible
- if YOU are using OpenVPN, please give 2.4_alpha2 a good beating
- and report issues to openvpn-devel@lists.sourceforge.net

Q&A

- any questions?
- (not about IKEv2, please)
- https://community.openvpn.net/
- https://github.com/OpenVPN/openvpn
- https://github.com/OpenVPN/openvpn/blob/master/Changes.rst
- https://github.com/OpenVPN/openvpn3