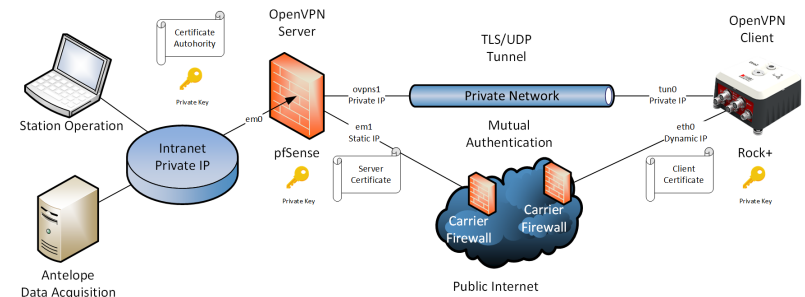


OpenVPN



ANTELOPE USER GROUP 2017, VIENNA

Stefan Radman

May 30, 2017

What is OpenVPN?

<https://en.wikipedia.org/wiki/OpenVPN>

2

OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls.

What is OpenVPN?

and what is it not?

- OpenVPN is a virtual private networking software
 - Open source (GPL)
 - Based on UDP/IP, TCP/IP (works through firewalls)
 - Certificate-based authentication (X.509)
 - Standard encryption cyphers (OpenSSL)
-
- OpenVPN is not IPsec
 - OpenVPN is not a firewall
 - OpenVPN is not proprietary



What is it good for?

Why should seismologist use it?

4

- Create trusted private networks over the Internet
- Protect traffic between datacenter and the digitizer
- Help secure access to remote sites
- Access to stations without static IP

How can I use it?

Platforms supporting OpenVPN

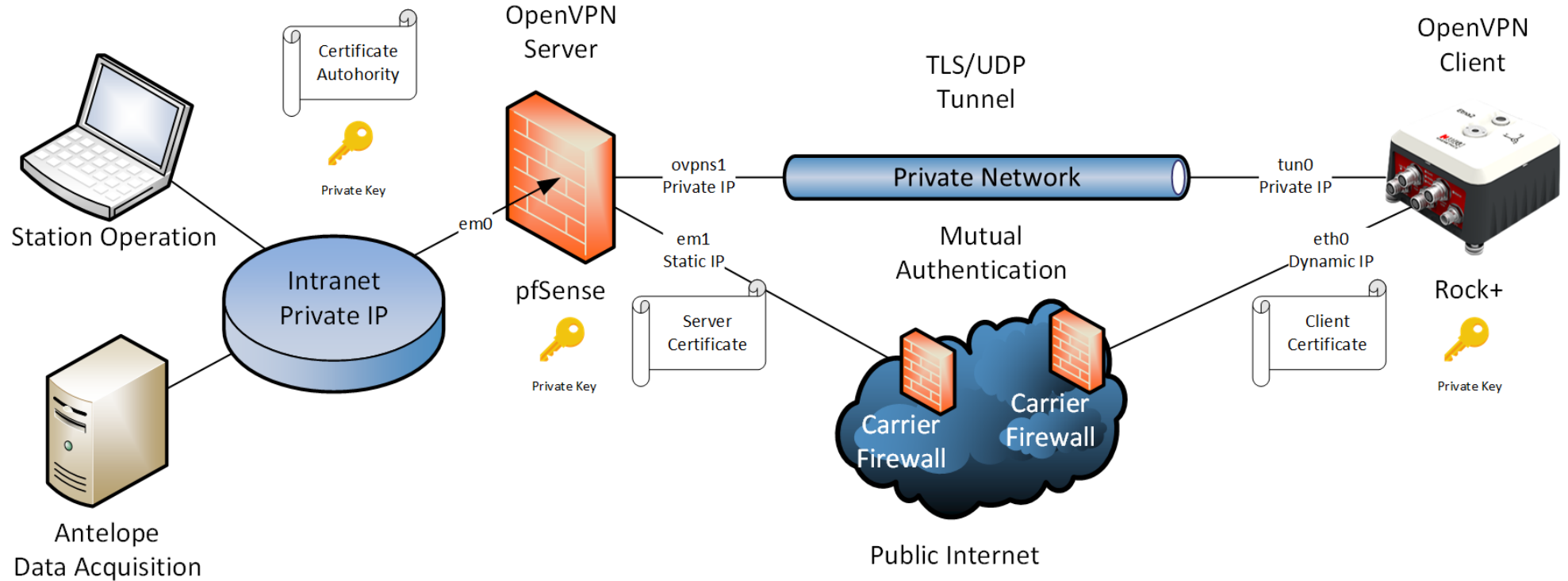
5

- Kinometrics Rock+ digitizers (Obsidian & Etna2)
- Cellular routers (e.g. Sierra Wireless, Conel)
- Installer packages for Linux, Mac, Windows
- Increasing number of network equipment vendors
- High degree of interoperability
- pfSense

OpenVPN using Certificates

OpenVPN tunnel to Rock+ digitizer

VIRTUAL PRIVATE NETWORK



PRIVATE TRANSPORT NETWORK

PUBLIC TRANSPORT NETWORK

- Packet filter firewall & router
- Open Source (Apache License 2.0)
- OpenVPN server & certificate management
- DHCP server, DNS proxy and much more
- BSD OS
- Easy installation from CD
- Web-based management

pfSense

User interface

Console menu

```
Message from syslogd@pfSense at May 30 06:19:11 ...
pfSense php-fpm: /index.php: Successful login for user 'admin' from:
FreeBSD/amd64 (pf.kmioss.com) (ttyv0)
*** Welcome to pfSense 2.3.4-RELEASE (amd64 full-install) on pf ***
WAN (wan)   -> em0   -> v4:
LAN (lan)   -> em1   -> v4:
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (ssh)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell
Enter an option: ^[[j^[[j^[[j^[[j
```

Web Interface

The screenshot shows the pfSense web interface dashboard. At the top, there is a navigation menu with options: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled "Status / Dashboard" and contains two primary sections: "System Information" and "Interfaces".

System Information:

Name	pf.kmioss.com
System	pfSense Serial: f81d7b07-441b-11e7-9093-005056829364 Netgate Unique ID: d9064efc513f4a28bae
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: 04/05/2016
Version	2.3.4-RELEASE (amd64) built on Wed May 03 15:13:29 CDT 2017 FreeBSD 10.3-RELEASE-p19 The system is on the latest version.
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU E5-2660 v2 @ 2.20GHz
Uptime	1 Day 03 Hours 38 Minutes 44 Seconds
Current date/time	Tue May 30 6:38:50 UTC 2017
DNS server(s)	• 127.0.0.1 • •
Last config change	Mon May 29 7:21:19 UTC 2017
State table size	0% (31/47000) Show states
MBUF Usage	3% (760/29666)
Load average	0.01, 0.04, 0.00
CPU usage	0%
Memory usage	29% of 477 MiB




Interfaces:

WAN	100baseT <full-duplex>
LAN	100baseT <full-duplex>

Certificate authority

System / Certificate Manager / CAs

CA's **Certificates** Certificate Revocation










Certificate Authorities					
Name	Internal	Issuer	Certificates	Distinguished Name	Actions
OpenVPN CA	✓	self-signed	2	emailAddress=smr@kmi.com, ST=California, OU=Open Systems and Services, O=Kinometrics Inc, L=Pasadena, CN=OpenVPN CA, C=US Valid From: Mon, 29 May 2017 03:10:43 +0000 Valid Until: Thu, 27 May 2027 03:10:43 +0000	  

[+ Add](#)

Client/Server certificates

System / Certificate Manager / Certificates

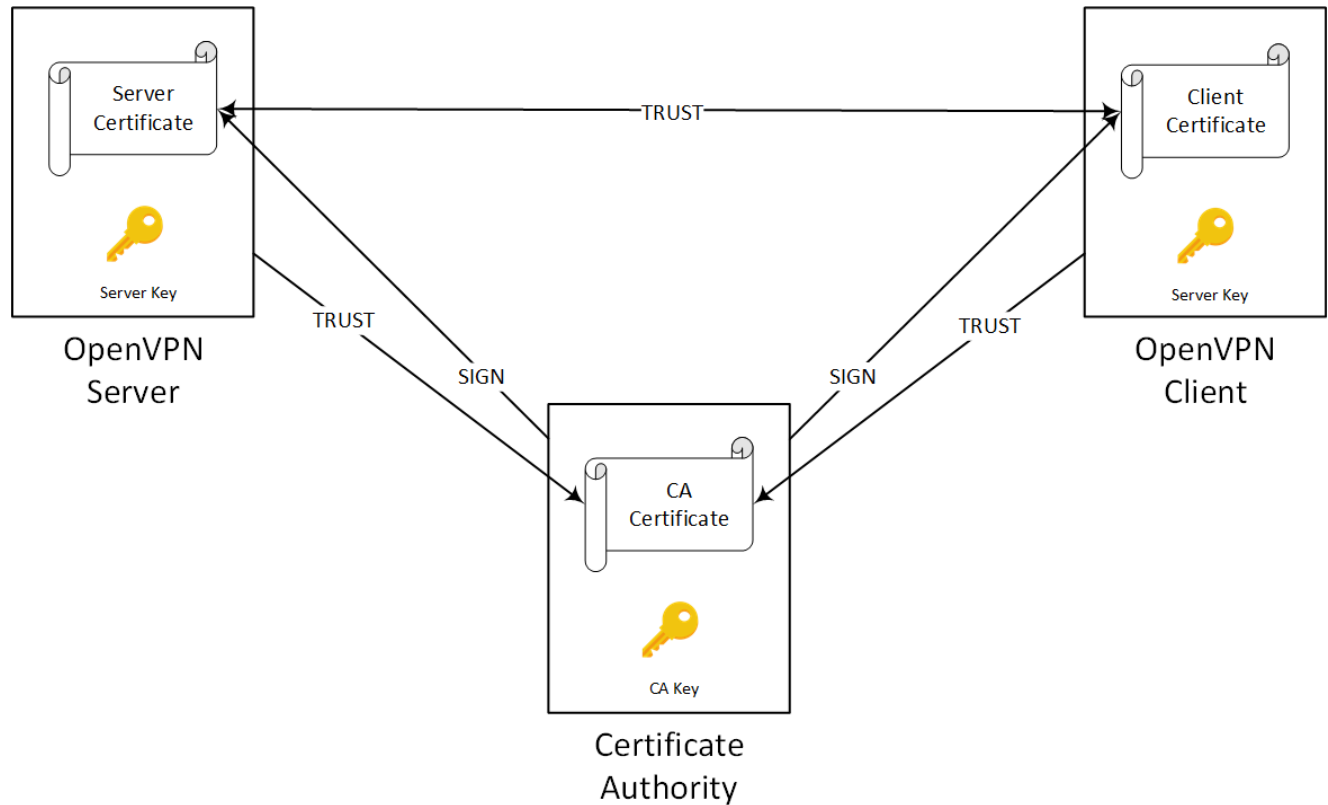
CA's **Certificates** Certificate Revocation

Certificates				
Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (592b8efd51610) Server Certificate CA: No, Server: Yes	self-signed	emailAddress=admin@pfSense.localdomain, ST=State, O=pfSense-592b8efd51610, C=US Valid From: Mon, 29 May 2017 03:01:17 +0000 Valid Until: Sat, 19 Nov 2022 03:01:17 +0000	webConfigurator	  
OpenVPN Server Server Certificate CA: No, Server: Yes	OpenVPN CA	emailAddress=smr@kmi.com, ST=California, OU=Open Systems and Services, O=Kinometrics Inc, L=Pasadena, CN=OpenVPN CA, C=US Valid From: Mon, 29 May 2017 03:24:02 +0000 Valid Until: Thu, 27 May 2027 03:24:02 +0000	OpenVPN Server	  
ETNA2 User Certificate CA: No, Server: No	OpenVPN CA	emailAddress=smr@kmi.com, ST=California, OU=Open Systems and Services, O=Kinometrics Inc, L=Pasadena, CN=ETNA2, C=US Valid From: Mon, 29 May 2017 03:42:38 +0000 Valid Until: Thu, 27 May 2027 03:42:38 +0000		  

[+ Add](#)

Certificates & trust relationship

How mutual trust is established



OpenVPN server

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

OpenVPN Servers				
Protocol / Port	Tunnel Network	Crypto	Description	Actions
UDP / 1194	192.168.20.0/24	Crypto: AES-256-CBC/SHA1 D-H Params: 2048 bits	OpenVPN Server (tun)	

[+ Add](#)

Client export

Servers configured with features that require OpenVPN 2.4 will not work with OpenVPN 2.3.x or older clients. These features include: AEAD encryption such as AES-GCM, TLS Encryption+Authentication, ECDH, LZ4 Compression and other non-legacy compression choices, IPv6 DNS servers, and more.

User	Certificate Name	Export
Certificate (SSL/TLS, no Auth)	ETNA2	<ul style="list-style-type: none"> - Standard Configurations: <ul style="list-style-type: none"> - Inline Configurations: <ul style="list-style-type: none"> - Current Windows Installer (2.4.2-1x01): <ul style="list-style-type: none"> - Old Windows Installers (2.3.15-1x01): <ul style="list-style-type: none"> - Viscosity (Mac OS X and Windows): <ul style="list-style-type: none"> - Yealink SIP Handsets: <ul style="list-style-type: none"> -

If a client is missing from the list it is likely due to a CA mismatch between the OpenVPN server instance and the client certificate, or the client certificate does not exist on this firewall.

OpenVPN 2.4 requires Windows Vista or later
 The "win6" Windows installers include a new tap-windows6 driver that works only on Windows Vista and later.
 The "XP" Windows installers work on Windows XP and later versions.

Links to OpenVPN clients for various platforms:

OpenVPN Community Client - Binaries for Windows, Source for other platforms. Packaged above in the Windows Installers
 OpenVPN For Android - Recommended client for Android
 FEAT VPN For Android - For older versions of Android
 OpenVPN Connect: Android (Google Play) or iOS (App Store) - Recommended client for iOS
 Viscosity - Recommended commercial client for Mac OS X and Windows

Rock+ OpenVPN

Firmware requirements & configuration

12

- Firmware support
 - Etna2 Linux Update > 1.2 (current = 1.3)
 - Obsidian Linux Update > 3.4 (current)
- Configuration
 - `/etc/openvpn/*.conf`
 - `service openvpn start`
 - `initdconfig openvpn start`

Rock+ Security

Netfilter requirements & configuration

13

- Firmware support
 - Etna2 Linux Update > 1.2 (current = 1.3)
 - Obsidian Linux Update > 3.3 (current = 3.4)
- Configuration
 - “Relaxed” mode: `kminetfilterdefaults`
 - “Stealth” mode: `kminetfilterstealth`

Rock/Rock+ Security

Reminder - Basic cybersecurity

14

- Change factory default passwords!!
- Use a firewall
- Block/disable unused services
- KMI Application Note #63

Basic Cyber Security

http://wiki.kmi.com/wiki/index.php/Rock_Application_Notes

OpenVPN platforms

Linux

15

- Linux
 - Binary openvpn packages included in most current Linux distributions (RHEL/CentOS, Debian, ...)
 - Install using native mechanism (yum, apt-get,..)
 - Supported in GNOME NetworkManager (including GUI)
 - Configuration via GUI or config files in /etc/openvpn



OpenVPN platforms

Windows/Mac

16

- Windows
 - Tunnelblick (free, with GUI)
- Mac
 - Tunnelblick (free)
 - Viscosity (commercial)
 - macports (no GUI)

Resources

OpenVPN/pfSense/Rock+/Etna2

17

OpenVPN

<http://www.openvpn.org>

pfSense

<http://www.pfsense.org>

Rock+/Etna2

<http://wiki.kmi.com/wiki/index.php/Rock>

OpenVPN

18

Thanks for listening!

Questions?