

Installationsanleitung
Serverbased OpenVPN-Management

Thorsten Robers
OpenSource Training Ralf Spenneberg
23. Januar 2009

Zusammenfassung

OpenVPN Management ist ein Werkzeug zur clientseitigen Steuerung und Verwaltung von OpenVPN-Tunneln. Es kann jedoch auch zur ausschließlichen Steuerung unterschiedlicher OpenVPN-Tunnel genutzt werden. Die serverbasierte Konfigurationsverteilung ist ein zusätzliches Feature, welches im Besonderen für Firmen zur Anbindung von AußendienstmitarbeiterInnen und zur Verteilung neuer Konfigurationsdateien konzipiert wurde.

Diese Dokumentation und Installationshinweise stellen einen kompakten Einstieg in die clientseitige Verwaltung von OpenVPN-Tunneln dar. Die Installation und Besonderheiten auf unterschiedlichen Plattformen werden im Rahmen dieser Dokumentation besprochen. Ebenso wird notwendiges Hintergrundwissen zur Administration der serverbasierten Konfigurationsverteilung vermittelt. Konfigurationseinstellungen für OpenVPN werden im Rahmen dieser Dokumentation nicht aufgezeigt. Hierzu wird die Website www.openvpn.net empfohlen.

Inhaltsverzeichnis

| | | |
|----------|---|-----------|
| 1 | Einleitung | 2 |
| 1.1 | Feature-Überblick | 2 |
| 1.2 | Prüfung der Systemintegrität | 2 |
| 1.3 | Serverbasierte Konfigurationsverwaltung | 3 |
| 1.4 | Voraussetzungen | 3 |
| 1.4.1 | OpenVPN Managementkonsole | 3 |
| 1.4.2 | Serverbasierte Konfigurationsverteilung | 4 |
| 2 | Technische Umsetzung | 5 |
| 2.1 | Allgemeines | 5 |
| 2.2 | Serverbasierte Konfigurationsverteilung | 6 |
| 2.3 | Serverbasierte Konfiguration des Werkzeuges | 6 |
| 2.3.1 | Log-Dateien | 6 |
| 2.3.2 | Konfigurationsverteilung | 6 |
| 3 | Installationshinweise | 7 |
| 3.1 | Windows XP und Windows Vista | 7 |
| 3.2 | Linux | 8 |
| 4 | Erster Programmstart | 9 |
| 5 | Besonderheiten auf den einzelnen Plattformen | 10 |
| 5.1 | Linux | 10 |
| 6 | Token und Smartcards anbinden | 11 |

Kapitel 1

Einleitung

Bei *serverbased OpenVPN-Management* handelt es sich in erster Linie um ein neues Konzept der zentralisierten Verwaltung von OpenVPN-Konfigurationen. Hierzu wurde ein Werkzeug entwickelt, welches zunächst nur für die clientseitige Verwaltung und Steuerung der einzelnen VPN-Tunnel verfügbar ist. Eine kurze Zusammenfassung der bisher implementierten Features finden Sie im folgenden Kapitel.

1.1 Feature-Überblick

Je nach verwendetem Betriebssystem stehen mehr oder weniger Features beim OpenVPN-Management-Werkzeug zur Verfügung. Auf die Besonderheiten der einzelnen Plattformen wird später eingegangen. Hier sollen nur die vorhandenen Features aufgelistet werden, ohne auf deren Verfügbarkeit auf unterschiedlichen Plattformen einzugehen.

- Steuerung (Auf- und Abbau) der einzelnen VPN-Tunnel
- Visualisierung des Tunnel-Status
- Prüfung der Systemintegrität vor Tunnelaufbau
- Serverbasierte Verteilung von OpenVPN-Konfigurationen
- Automatischer Start des OpenVPN-Dienstes bei Verwendung des Werkzeuges

1.2 Prüfung der Systemintegrität

Der Aufbau von OpenVPN-Tunnel zu anderen Rechnern oder Netzwerken ermöglicht einen sicheren Datenaustausch zwischen den beteiligten Kommunikationspartnern. Jedoch birgt diese Form der Datenübertragung auch Gefahren. So wird der verschlüsselte Datenverkehr durch OpenVPN nicht auf Viren, Trojaner, Würmer oder andere schädliche Software (z. B. Spionagesoftware) analysiert. Auch eine vorgeschaltete Firewall oder ein Intrusion Detection System (IDS) werden meist umgangen. Bisher bietet OpenVPN von Haus aus hierfür keine Lösung an.

Mit diesem Werkzeug besteht erstmals die Möglichkeit, vor dem Aufbau eines OpenVPN-Tunnel die Systemintegrität des Clients zu prüfen. Nur im Falle eines aktuellen und aktiven Virenschanners kann mit diesem Werkzeug eine Verbindung zu OpenVPN-Servern aufgebaut werden. Hierdurch wird ein enormer zusätzlicher Sicherheitsgewinn erzielt. ¹

1.3 Serverbasierte Konfigurationsverwaltung

Das *OpenVPN Management*-Werkzeug bietet die Möglichkeit, die Verwaltung von OpenVPN-Konfigurationen zu zentralisieren. Änderungen an der IT-Struktur (zusätzliche OpenVPN-Server, ...) oder Anpassungen von Konfigurationen von AußendienstmitarbeiterInnen an unterschiedliche Arbeitsplatzumgebungen werden somit enorm vereinfacht. Das vorgestellte Werkzeug übernimmt die vollständige clientseitige Verwaltung der OpenVPN-Konfigurationen. Somit muss kein Endanwender mit der händischen Verwaltung der VPN-Tunnel betraut werden. Die Verwaltung kann vollständig in die Hände fachkundiger Administratoren übergeben werden.

Das Werkzeug ist in der Lage anhand des CommonName von x509-Zertifikaten die benötigten Konfigurationsdateien herauszufiltern, herunterzuladen und anschließend den OpenVPN-Dienst zu starten, damit die neuen Konfigurationen direkt genutzt werden können.

Neben der Verteilung von OpenVPN-Konfigurationen kann auch das Werkzeug selbst zentral konfiguriert werden. Die technische Umsetzung der Konfigurationsverteilung wird ab Seite 5 im Kapitel 2 ausführlich vorgestellt.

1.4 Voraussetzungen

Für die reine Steuerung von OpenVPN-Tunnel werden keine wirklichen Voraussetzungen erwartet. OpenVPN muss auf dem System installiert und als Dienst startbar sein. In den Konfigurationen für die jeweiligen OpenVPN-Tunnel muss lediglich die Telnet-Managementschnittstelle konfiguriert werden.

1.4.1 OpenVPN Managementkonsole

Zur Konfiguration der Telnet-Managementschnittstelle müssen lediglich die folgenden 3 Zeilen in allen OpenVPN-Konfigurationen eingetragen werden.

```
management 127.0.0.1 <Port> [managepasswortdatei]
management-query-passwords
management-hold
```

Ohne diese 3 Zeilen lassen sich die OpenVPN-Tunnel nicht mit dem Werkzeug steuern. Mittels der ersten Zeile stellt die OpenVPN-Instanz eine Telnet-Schnittstelle unter der Adresse 127.0.0.1 und einem beliebigen freien Port ≥ 1024 zur Verfügung. Für jeden Tunnel ist ein anderer Port zu wählen. Optional kann

¹Jedoch wird dieser Sicherheitsgewinn nur mit der Verwendung des vorgestellten Werkzeuges erreicht. Werden direkt mit der durch OpenVPN zur Verfügung gestellten Telnet-Managementschnittstelle die VPN-Tunnel aufgebaut, wird keine Systemintegritätsprüfung durchgeführt.

für den Zugriff auf die Schnittstelle ein Passwort gesetzt werden. Das Passwort wird relativ zum Konfigurationsverzeichnis in einer ASCII-Datei abgelegt. Der entsprechende relative Pfad auf die Datei ist anzugeben.

Die zweite Zeile veranlasst die OpenVPN-Instanz dazu, mögliche Passphrasen für Zertifikate oder sonstige Authentifizierungen an die Telnet-Schnittstelle durchzureichen.

Abschließend wird mit der dritten Zeile dafür gesorgt, daß der Tunnel zwar instanziiert, jedoch nicht automatisch aufgebaut wird. Auf- und Abbau des Tunnel übernimmt dann das Werkzeug.

1.4.2 Serverbasierte Konfigurationsverteilung

Um die zentrale Konfigurationsverteilung einzusetzen wird lediglich ein SSL-fähiger Webserver benötigt, auf dem die OpenVPN-Konfigurationen, ebenso wie die Konfigurationen für das Werkzeug, selbst hinterlegt werden können. Ein SSL-fähiger Webserver wird benötigt, damit zum Einen eine Authentifizierung des Webservers vorgenommen werden kann. Zum anderen werden die Konfigurationsdateien verschlüsselt übertragen und somit weitestgehend vor Fremden Augen geheimgehalten. Zur Erhöhung des Schutzes der Konfigurationsdateien können die Verzeichnisse auf dem Webserver durch eine zusätzliche Authentifizierung vor fremden Zugriff geschützt werden.

Der Anwender benötigt für diesen Vorgang ein gültiges Zertifikat für seinen OpenVPN-Zugang. Anhand dieses Zertifikates kann das Werkzeug entscheiden, welche Konfigurationen für den Anwender verwendet werden sollen. Somit wird es Anwendern, die lediglich mit Zertifikat und Werkzeug ausgestattet sind, ermöglicht OpenVPN-Konfigurationen selbstständig zu installieren.

Kapitel 2

Technische Umsetzung

Im Folgenden sollen die technischen Grundlagen der Konfigurationsverwaltung vorgestellt werden. Hierbei wird die serverseitige Bereitstellung von Konfigurationen beschrieben. Bisher gibt es für die automatisierte Erstellung und serverseitige Verwaltung der Konfigurationsdateien kein Werkzeug oder Webinterface. Dieses wird jedoch von uns perspektivisch entwickelt und zur Verfügung gestellt werden.

2.1 Allgemeines

Alle Konfigurationen müssen in einer zentralen ASCII-Datei `updates.txt` bekanntgemacht werden. Diese Datei ist die Grundlage für die clientseitige Konfigurationsaktualisierung. Der Aufbau der Datei ist einfach. Jede Konfigurationsdatei wird durch eine eigene Zeile repräsentiert. Die einzelnen Felder werden durch `:` von einander getrennt.

```
*:*/openvpn/vpnclient01.conf:8e80c1c9ad0137cdff563ee4b6418435
*:fensterblick:/openvpn2/test2.conf:1efcbd2b3540f37ca4bfb38f6b686605
$:strandblick:/openvpn/gui.conf:4eba4805078d910059f9f17f568b6581
$:fensterblick:/openvpn2/gui.conf:e78a480acb8d952059f9fe4356f46574
```

Die erste Spalte gibt Aufschluss darüber, ob es sich um eine OpenVPN-Konfigurationsdatei oder um eine Konfigurationsdatei für das Werkzeug handelt. Ein `*` steht für OpenVPN-Konfigurationen. Konfigurationen für das Client-Werkzeug werden mit `$` eingeleitet.

Die zweite Spalte gibt Aufschluß darüber für welche Anwender die jeweilige Konfigurationsdatei bereitgestellt wird. Hierbei kann mittels `*` eine Wildcard für alle Anwender verwendet werden. Ansonsten muss hier der CommonName des jeweiligen x509-Zertifikates verwendet werden.

In der dritten Zeile wird der Ort der Konfigurationsdatei angegeben. Er wird relativ zur Domain des Updateservers angegeben. Liegt die Datei beispielhaft unter `https://software.opensource-security.de/openvpn/test.conf`, müsste in diesem Fall `/openvpn/test.conf` angegeben werden.

Die letzte Spalte ist ein md5-Hash über die Datei, anhand dessen das *OpenVPN Management*-Werkzeug erkennen kann, ob sich die Konfiguration seit dem letzten Start des Werkzeuges geändert hat und somit aktualisiert werden muss.

2.2 Serverbasierte Konfigurationsverteilung

Die OpenVPN-Konfigurationen werden wie üblich als ASCII-Dateien in den entsprechenden Verzeichnissen und mit den entsprechenden Dateinamen auf dem Webserver gespeichert. Im Anschluss müssen diese Dateien in der `updates.txt` bekanntgemacht werden.

2.3 Serverbasierte Konfiguration des Werkzeuges

Für die Konfiguration des Werkzeuges wird ebenfalls eine ASCII-Datei verwendet. Die Datei hat einen simplen Aufbau. Zu dem jeweiligen Keyword wird durch `:` getrennt der entsprechende Wert definiert.

2.3.1 Log-Dateien

Es können unterschiedliche Teile des Werkzeuges konfiguriert werden. Für die Möglichkeit Log-Nachrichten des Werkzeuges und der OpenVPN-Tunnel an die Systemadministratorin oder den Systemadministratoren zu verschicken können Konfigurationen wie folgt vorgenommen werden:

```
mailserver:smtp.server.de
mailusername:mailuser
mailaddress:mailuser@firma.de
mailto:admin@firma.de
```

2.3.2 Konfigurationsverteilung

Für Einstellungen der Konfigurationsverteilung gibt es die beiden folgenden Keywords.

```
updateserver:https://openvpn-update.firma.de
auto-update:true
configuration_files:/etc/openvpn/
```

Bei `updateserver` wird der Server, auf dem die Konfigurationen abgelegt sind angegeben. Bei `auto-update` kann wahlweise `true` oder `false` angegeben werden. Mit `configuration_files` wird das Verzeichnis, in dem sich die OpenVPN-Konfigurationen befinden definiert.

Kapitel 3

Installationshinweise

Das Werkzeug wurde auf Basis des .NET-Frameworks entwickelt. Daher ist es unter allen MS Windows-Plattformen mit wenigstens .NET 2.0 lauffähig. Ebenso unterstützt es allen weiteren Plattformen, auf denen die OpenSource Implementierung des .NET-Frameworks *Mono* läuft. Dies sind momentan alle aktuellen Linux-Distributionen und MacOSX. Allen Betriebssysteme nutzen die selben Binaries. Dennoch gibt es noch Unterschiede in den Funktionalitäten des Werkzeuges (siehe Kapitel 5) auf unterschiedlichen Betriebssystemen.

3.1 Windows XP und Windows Vista

Für die MS Windows-Plattformen wird ein Installer zur Verfügung gestellt. Mittels dieses Installers lässt sich das Tool und wenn noch nicht vorhanden automatisch die benötigte .NET-Version installieren.

Für die Ausführung des Werkzeuges wird eine Installation der aktuellen Version von OpenVPN (www.openvpn.net) vorausgesetzt. Unter Windows Vista muss zwingend die OpenVPN-Version 2.1 installiert werden, da ältere Versionen nicht unter Vista laufen. OpenVPN sollte unter beiden Plattformen nicht in den Ordner Programme, sondern direkt unterhalb des Root-Verzeichnisses installiert werden. Andernfalls wird es zu Problemen mit dem automatischen Update der Konfigurationsdateien für die OpenVPN-Tunnel kommen.

Der Administrator muss nach der Installation der benötigten Programme noch die Rechte zur Steuerung des OpenVPN-Dienstes anpassen. Für alle Anwender müssen mittels `subinacl`¹ die Rechte zum Starten und Stoppen gesetzt werden. Der Befehl hierzu könnte beispielhaft wie folgt aussehen:

```
subinacl /SERVICE ‘‘OpenVPNService’’ /GRANT=john=TO
```

Nach der Installation von OpenVPN, eventuell .NET und dem neuen Werkzeug, sollten alle notwendigen Programme installiert sein. So das sie nur noch eine Ersteinrichtung (siehe Kapitel 4) des Werkzeuges vornehmen müssen. Die Konfigurationen für die OpenVPN-Zugänge lassen sich dann automatisch herunterladen. Sollten Sie diese nicht wünschen, so erstellen Sie ihre OpenVPN-Konfigurationen selbstständig.

¹<http://www.microsoft.com/downloads/details.aspx?FamilyID=e8ba3e56-d8fe-4a91-93cf-ed6985e3927b&displaylang=en>

3.2 Linux

Unter Linux reicht es aus über die jeweilige Paketverwaltung der Distribution OpenVPN und Mono zu installieren.

Sie können für das Werkzeug einfach die selben Binaries verwenden, die sie auch unter MS Windows-Plattformen starten.

Für den automatischen Start und Neustart des OpenVPN-Dienstes müssen die Berechtigungen für die Ausführung des OpenVPN-Startskriptes gesetzt werden. Hierzu wird auf *sudo* zurückgegriffen, mit dessen Hilfe beliebige Anwenderinnen und Anwender temporär mehr Rechte erhalten. Konfigurieren Sie also für die jeweiligen NutzerInnen die Berechtigung wie folgt:

```
thorsten    ALL=NOPASSWD:/etc/init.d/openvpn restart
```

Das editieren der sudo-Konfigurationsdatei erfolgt mit dem Werkzeug *visudo* als Root.

Für das automatische Update der OpenVPN-Konfigurationen müssen ebenfalls Datei- und Verzeichnisberechtigungen angepasst werden. Erstellen sie hierzu eine neue Gruppe OpenVPN und erteilen dieser Gruppe den schreibenden Zugriff auf das gesamte Verzeichnis `/etc/openvpn/` inklusive aller Unterverzeichnisse. Anschließend werden die AnwenderInnen, die das Werkzeug benutzen dieser Gruppe zugeteilt.

Kapitel 4

Erster Programmstart

Beim ersten Starten des Programms können nur die aktuell bereits vorhanden und entsprechend konfigurierten (vgl. Kapitel 1.4.1) OpenVPN-Tunnel gesteuert werden.

Für alle weiteren Features sind weitergehende Konfigurationen am Werkzeug notwendig. Wie bereits in Kapitel 2.3 ausgeführt können diese Vorgaben auch über einen zentralen Server vorgenommen werden. Dieser Updateserver muss dem Werkzeug zumindest beim ersten Programmstart einmalig bekannt gemacht werden. Hierzu ist unter den Einstellungen ein Reiter mit der Bezeichnung “Update” zu finden. Hier können die Vorgaben für den Updateserver und für automatische Updates gemacht werden. Zusätzlich muss für das automatische Update auch ein Verweis auf die Zertifikatsdatei, die sich hinter dem Reiter “Files” verbirgt, erfolgen.

Beim nächsten Start wird das Werkzeug automatisch ein Update der bestehenden Konfigurationen durchführen. Hierbei wird sowohl das Werkzeug selbst, als auch die vorhandenen OpenVPN-Konfigurationen aktualisiert oder ergänzt.

Ist das automatische Update nicht gewünscht, dann lässt es sich einfach durch das Entfernen des Häkchen bei “auto-update” abschalten.

Kapitel 5

Besonderheiten auf den einzelnen Plattformen

Auch wenn das Werkzeug in .NET/mono entwickelt wurde und somit auf vielen unterschiedlichen Betriebssystemen lauffähig ist, gibt es dennoch gravierende Unterschiede in Abhängigkeit von der verwendeten Plattform. Während ein Feature auf der einen Plattform einfach zu implementieren ist, stellt sich die Realisierung des selben Feature auf einer anderen Plattform als sehr komplex dar. Generell verfolgen wir den Ansatz alle Feature auf allen Systemen zur Verfügung zu stellen. Dennoch haben wir uns bereits zum jetzigen Zeitpunkt für eine erste Veröffentlichung entschieden. Die Unterschiede zwischen den verschiedenen Plattformen wollen wir daher hier im Folgenden dokumentieren.

5.1 Linux

Unter den unterschiedlichsten Linux-Derivaten wird bisher keine Prüfung der Systemintegrität vorgenommen. Die Prüfung der Existenz, Aktualität und Aktivität eines Virenschanners wird bisher nur unter den unterschiedlichen MS Windows-Plattformen unterstützt.

Kapitel 6

Token und Smartcards anbinden

Der OpenVPN Management-Client unterstützt vollständig die Einbindung von Smartcards und Token zur Authentifizierung von OpenVPN-Verbindungen. Hierzu ist die Installation von OpenSC erforderlich. Unter Windows befindet sich dieses in einem Bundle mehrerer Programme. Welches unter <http://www.opensc-project.org/files/scb/> zu finden ist. Unter Linux verwenden Sie die Paketverwaltung zur Installation von OpenSC.

Anschließend können sie die Smartcard für den Einsatz mit OpenVPN und dem Management-Client einrichten. Hier wird nur ein Abstract einer ausführlichen Dokumentation von <http://michele.pupazzo.org/docs/smart-cards-openvpn.html> vorgestellt.

Zunächst muss eine PKCS15-Struktur auf dem Crypto-Chip eingerichtet werden.

```
# pkcs15-init -E
Transport key (External authentication key #1) required.
Please enter key in hexadecimal notation (e.g. 00:11:22:aa:bb:cc),
or press return to accept default.
```

```
To use the default transport keys without being prompted,
specify the --use-default-transport-keys option on the
command line (or -T for short), or press Ctrl-C to abort.
Please enter key [2c:15:e5:26:e9:3e:8a:19]:
```

```
$ pkcs15-init --create-pkcs15
Please enter Security Officer PIN:
Please type again to verify:
Unblock Code for New User PIN (Optional - press return for no PIN).
Please enter User unblocking PIN (PUK):
Please type again to verify:
Transport key (External authentication key #1) required.
Please enter key in hexadecimal notation (e.g. 00:11:22:aa:bb:cc),
or press return to accept default.
```

To use the default transport keys without being prompted, specify the `--use-default-transport-keys` option on the command line (or `-T` for short), or press `Ctrl-C` to abort. Please enter key `[2c:15:e5:26:e9:3e:8a:19]`:

```
$ pkcs15-init --store-pin --auth-id 01 --label "<Name des Inhabers>"
New User PIN.
Please enter User PIN:
Please type again to verify:
Unlock Code for New User PIN (Optional - press return for no PIN).
Please enter User unblocking PIN (PUK):
Please type again to verify:
Security officer PIN required.
Please enter Security officer PIN:
Transport key (External authentication key #1) required.
Please enter key in hexadecimal notation (e.g. 00:11:22:aa:bb:cc),
or press return to accept default.
```

To use the default transport keys without being prompted, specify the `--use-default-transport-keys` option on the command line (or `-T` for short), or press `Ctrl-C` to abort. Please enter key `[2c:15:e5:26:e9:3e:8a:19]`:

Im Anschluß an die grundlegende Einrichtung des Token können sie die mit beispielsweise *easy-rsa* erstellen Zertifikate und Keys auf den Token übertragen. Bedenken Sie, dass sie mit *easy-rsa* eine `pkcs12`-Struktur für ihre Zertifikate verwendet haben. Hierzu wird ein entsprechendes Skript zur Verfügung gestellt.

```
$ pkcs15-init -S client-cert.p12 -f PKCS12 -a 01
error:23076071:PKCS12 routines:PKCS12_parse:mac verify failure
Please enter passphrase to unlock secret key:
Importing 2 certificates:
 0: /C=IT/ST=Bozen/L=Sterzing/O=Foo/CN=Michele/emailAddress=michele@pupazzo.org
 1: /C=IT/ST=Bozen/L=Sterzing/O=Foo/CN=CA VPN/emailAddress=ca@pupazzo.org
Security officer PIN required.
Please enter Security officer PIN:
User PIN required.
Please enter User PIN:
Security officer PIN required.
Please enter Security officer PIN:
```

Damit sollten die Smartcard oder der Token für den Einsatz mit OpenVPN eingerichtet sein. Die weitere Konfiguration von OpenVPN entnehmen sie der Dokumentation für OpenVPN.