revobox office

Installationsanleitung

Software Release 1.16

Die aktuellste Version dieser Installationsanleitung ist verfügbar unter:
http://www.revosec.ch/files/revobox-manual.pdf

Lieferumfang

Im Lieferumfang der revobox sind enthalten:

- revobox
- Netzteil 18V DC
- Patchkabel RJ-45 25cm
- Installationsanleitung

Anforderungen

Für den Betrieb der revobox im lokalen Netzwerk wird ein DHCP-Server empfohlen und ist für die Installation sogar erforderlich. Dieser Dienst wird in den meisten Installationen vom Internet-Router erbracht.

Die revobox wurde für den Einsatz hinter einem NAT-Router konzipiert. Dieser muss UDP-Ports weiterleiten können. Bei einem UPnP-fähigen Router geschieht dies automatisch, andernfalls ist eine manuelle Einrichtung auf dem Router notwending.

Clientseitig wird mindestens eine beliebige Version von Windows® 7 oder Mac OS X 10.7vorausgesetzt, um den integrierten VPN-Client zu verwenden. Ältere Versionen von Windows® werden nicht direkt unterstützt, der Einsatz von Drittprodukten st aber möglich. Unter Linux kann strongSwan eingesetzt werden. iOS-Geräte ab Version 5 werden unterstützt. Die Unterstützung von Android ab Version 4 ist gegeben, hängt jedoch auch von der Hersteller-spezifischen Umsetzung ab.

Für die Authentisierung gegenüber einem RADIUS-Server wird ein nach RFC2865 kompatibler Server benötigt. Im Zusammenhang mit einem Active Directory® kann IAS oder NPS eingesetzt werden. Um Nutzer über die SuisseID zu authentisieren wird eine gültige SuisseID von einem anerkannten Anbieter benötigt.

Sicherheitshinweise

Beachten Sie folgende Sicherheitshinweise vor der Installation und Inbetriebnahme der revobox:

- Installieren und verwenden Sie die revobox nur innerhalb von Gebäuden.
- Verwenden Sie nur das mitgelieferte Netzteil und das mitgelieferte Netzwerkkabel für den Anschluss der revobox.
- Trennen Sie die revobox während eines Gewitters vom Netzwerk und vom Stromnetz.
- Öffnen Sie das Gehäuse der revobox nicht.
- Installieren Sie die revobox nicht auf wärmeempfindlichen Flächen, da sich das Gerät im Betrieb erwärmen kann.
- Achten Sie auf genügend Abstand zu Störungsquellen wie Mikrowellen oder anderen Elektrogeräten.
- Vermeiden Sie die Installation in der nähe von Heizkörpern oder anderen Wärmequellen und vermeiden Sie direkte Sonneneinstrahlung.
- Schützen Sie das Gerät vor Flüssigkeiten und zu hoher Feuchtigkeit.
- Definieren Sie lediglich starke Passwörter von mindestens acht Zeichen Länge, bestehend aus einer Mischung von Klein- und Grossbuchstaben, Zahlen und Sonderzeichen.
- Bewahren Sie niedergeschriebene Passwörter nur an sicheren Orten auf und wechseln Sie Passwörter regelmässig.

Anschlüsse

Die *revobox* ist auf der Rückseite mit folgenden Anschlüssen ausgestattet:

1 2 3 4 5

1 Serieller RS-232 Anschluss (Terminal)
2 Fast Ethernet RJ-45 Anschluss
3 Fast Ethernet RJ-45 Anschluss
4 USB-Anschluss (x2)
5 Stromversorgung DC 18V

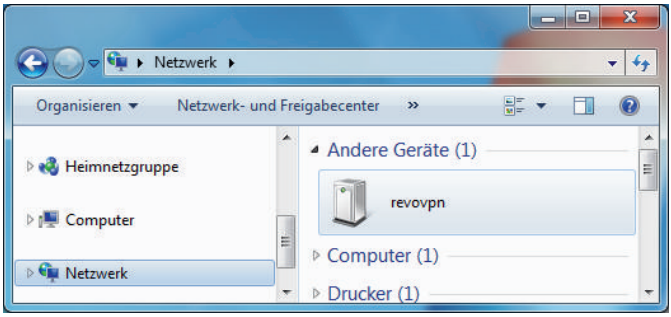
Der Serielle Anschluss (1) erlaubt den Terminal-Zugriff auf das Gerät mit Hilfe eines Nullmodem-Kabels für Wartungszwecke. Der erste Fast Ethernet-Port (2) sowie die USB-Anschlüsse (4) sind in der jetzigen Software-Version ungenutzt, sie werden allenfalls für zukünftige Funktionen verwendet.

Der Fast Ethernet-Port (3) neben den USB-Anschlüssen wird für die Verbindung ins Netzwerk verwendet. Verbinden Sie diesen mit dem beiligenden RJ-45-Kabel mit einem LAN-Anschluss am NAT-Router oder einem damit verbundenen Ethernet-Switch. Der Port ist Auto MDI/MDX-fähig und kann mit gekreuztem oder ungekreuztem Kabel an einen MDI- oder MDX-Port angeschlossen werden.

Schliessen Sie das beigelegte Netzteil am DC-Anschluss (5) an und verbinden Sie es mit einer Steckdose.

Geräte-Konfiguration

Wurde das Gerät an das lokale Netzwerk angeschlossen, erscheint nach ca. 25s in der Netzwerkumgebung die revobox. Sollte sie nicht erscheinen, aktualisieren Sie die Ansicht und überprüfen allenfalls die Verkabelung.



Durch einen Doppelklick wird das Webinterface der revobox geöffnet. Vor der ersten Anmeldung muss ein Passwort gesetzt werden. Dieses Passwort wird für künftige Administrationsarbeiten am Gerät notwendig sein.

Nach der Anmeldung kann im Reiter *Gerät* der Status der revobox geprüft werden. Der DNS-Eintrag sollte nun auf die externe Adresse des NAT-Routers auflösen. Wenn kein zu Universal Plug and Play (UPnP) kompatibler Router gefunden wurde, oder die automatische Port-Weiterleitung nicht eingerichtet werden konnte, muss dies manuell am NAT-Router geschehen. Konsultieren Sie dazu die Dokumentation des Routers und richten Sie eine Port-Weiterleitung für die UDP Ports 500 und 4500 zur revobox ein. Die interne IP-Adresse der revobox ist über die *Eigenschaften* der revobox in der Netzwerkumgebung ersichtlich.

Standardmässig verwendet die revobox DHCP für die Adresskonfiguration. Die Konfiguration einer statischen Adresse ist über den Reiter *Gerät* möglich, dafür ist jedoch eine initiale Konfiguration über einen DHCP-Server erforderlich.

Benutzerkonten

Im Reiter *Benutzerkonten* können für einzelne Nutzer Konten eingerichtet und verwaltet werden. Es empfiehlt sich für jeden Nutzer ein separates Konto zu eröffnen, da ein einzelnes nicht für simultane Verbindungen verwendet werden kann.

Für die Authentisierung mittels Passwort kann ein Benutzername und ein Kommentar definiert werden. Der Kommetar hat keine weitere Bedeutung, kann aber bei der Verwaltung der Konten behilflich sein. Das Konto kann nach fünf Login-Versuchen gesperrt werden. Dies ist vor allem bei schwächeren Passwörtern empfehlenswert, damit ein dritter am Durchprobieren von Passwörtern scheitert.

Bei der Einrichtung eines Kontos für die SuisseID ist die SuisseID-Nummer erforderlich. Diese kann den Unterlagen zur jeweiligen SuisseID entnommen werden. Alternativ können Sie auch zuerst das VPN-Profil auf dem Client einrichten und die Verbindung für das noch nicht existierende Konto starten: Bei angeschlossener SuisseID erscheint die Nummer bei der PIN-Eingabe. Das Kommentarfeld kann wiederum für eigene Bemerkungen verwendet werden, wie etwa den Inhaber der SuisseID.

Für die Authentisierung gegen einen externen RADIUS-Server, wie etwa für Active-Directory®, muss die Server-Adresse sowie das RADIUS-Passwort definiert werden. Die revobox benutzt als NAS-Identifier *revobox* und leitet die EAP-Authentisierung vom Client an den Server weiter. Das einrichten eines Windows® Server für die RADIUS-Authentisierung entnehmen Sie bitte der separaten Dokumentation[1].

1 RADIUS für Windows® Server: http://www.revosec.ch/files/windows-radius.pdf

VPN-Profil auf Windows® 7 einrichten

Für die Client-Konfiguration steht ein Assistent zur Verfügung, welcher den Vorgang automatisiert. Er bezieht das öffentliche Gerätezertifikat von einem Server der revosec und richtet das VPN-Profil systemweit ein. Die Ausführung des Assistenten benötigt Administrator-Rechte. Der Konfigurations-Assistent kann über den Reiter *Gerät* des Webinterfaces der revobox oder die revosec Webseite bezogen werden[1].

Der Assistent verlang bei der Einrichtung die achtstellige, alphanumerische Bezeichnung der revobox. Diese ist auf der revobox vermerkt, im Reiter *Gerät* ersichtlich, oder sie kann in der Netzwerkumgebung über die *Eigenschaften* der revobox eingesehen werden.

Das sogenannte Split-Tunneling erlaubt es, lediglich den Verkehr zum Zielnetz über den Tunnel zu leiten. Der Kommunikation mit dem Internet erfolgt bei aktiviertem Split-Tunneling direkt und unverschlüsselt. Wenn Sie für diesen Rechner eine Anmeldung über die SuisseID beabsichtigen, setzen Sie die entsprechende Option im Assistenten.

Ist die Einrichtung mit dem Assistent erfolgt, wird dieser nicht mehr benötigt und kann gelöscht werden.

Die VPN-Verbindung kann nun über das Netzwerk-Trayicon unten rechts gestartet und wieder beendet werden. Nach dem ersten Verbinden erscheint nach wenigen Sekunden ein Dialog für die Auswahl des Netzwerkortes. Wählen Sie Heimnetzwerk, um wie gewohnt auf Dateifreigaben zugreifen zu können. Die Verbindung kann in den Adaptereinstellungen des Netzwerk- und Freigabecenters gelöscht oder nach Bedarf umbenannt werden.

Da die Verbindung systemweit konfiguriert wird, kann sie auch noch vor der Windows®-Anmeldung gegen einen Domain-Controller gestartet werden. Die Option zum Netzwerk Login erscheint bei Windows® 7 unten rechts im Anmeldedialog durch Benutzer wechseln.

1 revobox VPN-Profil Assistent: https://master.revosec.net/installer/revo-installer.exe

VPN-Profil unter Android 4 einrichten

Die revobox unterstützt Mobiltelefone und Tablets, welche unter Android 4.0 oder höher laufen. Diese Anleitung beschreibt die Verwendung der offiziellen strongSwan Android App, da der integrierte Android VPN Client einigen Einschränkunen unterliegt.

Die entsprechende App kann via Google Play Store über eine Suche nach *strongSwan* kostenlos installiert werden.

Um eine Verbindung zu einer revobox herzustellen, muss für die Überprüfung des Geräte-Zertifkates das revosec Root-Zertifikat installiert werden. Im Android-Browser ist dazu folgende URL aufzurufen:

*https://www.revosec.*ch/files/ca.crt

Nach der Eingabe eines beliebigen Namens muss die Installation allenfalls mit dem Passwort/PIN für das Android-Gerät bestätigt werden.

Nun kann in der strongSwan App ein neues Profil eingerichtet werden. Der *Gateway* besteht aus der eindeutigen Geräte-ID der revobox, ergänzt um *.revosec.net*, etwa *ZZZZZZZZ.revosec.net*. Als *Typ* ist *IKEv2 EAP (Benutzername/Passwort)* zu wählen, der *Benutzername* entspricht dem Benutzernamen des Kontos, welches auf der revobox eingerichtet wurde.

Es wird empfohlen, das CA-Zertifikat nicht automatisch zu wählen, sondern explizit das *revosec AG* CA-Zertifkat im Reiter *Benutzer* auszuwählen.

Die Verbindung kann nun in der Hauptansicht der App gestartet und gestoppt werden.

VPN-Profil unter iOS (iPhone/iPad) einrichten

Die VPN-Konfiguration für die revobox kann über eine *.mobileconfig*-Datei automatisiert auf einem iOS-Gerät eingerichtet werden. Der Besuch der URL

https://master.revosec.net/ZZZZZZZZ.mc

auf dem iPhone/iPad generiert eine Konfiguration, welche die VPN-Verbindung nach der Bestätigung einrichtet. *ZZZZZZZZ* ist dabei durch die Geräte-ID der revobx zu ersetzen.

VPN-Profil unter Mac OS X einrichten

Für die Konfiguration der VPN-Verbindung unter Mac OS X steht ein Konfigurations-Assistent[2] zur Verfügung. Dieser kann über den Reiter *Gerät* im Webinterface der revobox oder über die Webseite der revosec bezogen werden.

Bei der Ausführung des Assistenten ist die Geräte-ID der revobox anzugeben. Diese ist auf der revobox oder im Webinterface im Reiter *Gerät* einsehbar. Die Installation der Konfiguration benötigt Administratoren-Rechte.

Nach der Installation steht die Verbindung unter *Systemeinstellungen -> Netzwerk* zur Verfügung. Alternativ kann in der Verbindungsdefinition der VPN-Status in der Menu-Leiste angezeigt werden. Über das Icon ist das Aufbauen und Schliessen der VPN-Verbindung ebenfalls möglich.

2 revobox VPN-Profil OS X: http://master.revosec.net/installer/revo-installer.app.zip

Netzwerke koppeln

Durch den Zusammenschluss von mehreren revoboxen können einzelne Netzwerke zu einem Verbund zusammengeschlossen werden. Somit ist auf den Endgeräten in diesen Netzen keine VPN-Verbindung mehr einzurichten, alle Geräte in einem Netz können auf die Geräte in einem gekoppelten Netz zugreiffen. Das Einrichten von Netzkopplungen erfordert Kentnisse von IP-Netzwerken, es ist allenfalls ein Fachmann beizuziehen.

Um zwei Netzwerke zu koppeln muss in jedem eine revobox installiert sein. Diese bauen gegenseitig eine Verbindung auf und vermitteln zwischen den Netzwerken.

Damit gekoppelte Netze als ein gemeinsames agieren, empfiehlt es sich, alle Teilnetze zu einer gemeinsamen Broadcast-Domain zusammenzufassen. Dies ermöglicht das einfache Auffinden von Servern und Diensten auch in entfernten Netzen über Broadcast- und Multicast-Protokolle. Zwar ist es auch möglich, separate Broadcast-Domains beizubehalten, dies erfordert jedoch auf allen Geräten spezielle Routen, zudem funktionieren LAN-Protokolle nur eingeschränkt. Im Folgenden wird lediglich die Konfiguration mit einer gemeinsamen Broadcast-Domain beschrieben.

Wählen Sie für die zu koppelnden Netze ein gemeinsames Subnetz, wie etwa 10.0.0.0/16. In jedem Netz gilt in diesem Beispiel die Subnetzmaske 255.255.0.0. Dieser Adressbereich ist in die einzelnen Netze aufzuteilen, wie etwa 10.0.0.0/24, 10.0.1.0/24 usw. Dabei dürfen sich die Adressbereiche keinesfalls überlappen. In jedem Netzwerk wird dem Internet-Router eine Adresse aus dem lokalen Adressbereich zugeilt, der DHCP-Server vergibt Adressen aus demselben Bereich. Dieser soll jedoch eine Subnetmaske von 255.255.0.0 verteilen, damit alle Geräte eine gemeinsame Broadcast-Adresse von 10.0.255.255 verwenden.

Um die Netze zu koppeln wird im Reiter Netze gegenseitig die Geräte-ID der zu koppelnden revoboxen eingetragen. Als Freigabe ist der lokale Adressbereich zu definieren, oder auch nur einen Teil davon. Nach der Konfiguration verbinden sich die revoboxen automatisch und vermitteln zwischen den Netzwerken.

Hinweise zum Datenschutz

Für den Betrieb des DNS-, Update- und Konfigurations-Service hält die revosec folgende Informationen zu jeder revobox in einer zentralen Datenbank:

- Eindeutige, achtstellige Geräte-ID der revobox
- Aktuelle öffentliche IP-Adresse des Internet-Anschlusses
- Zeitstempel der letzten Aktualisierung der IP-Adresse
- Öffentliches Gerätezertifikat der revobox
- Aktuelle Software-Version

Die revosec kann für Support-Zwecke in einer separaten Datenbank Kontaktinformationen zur achtstelligen Geräte-ID speichern.

Die genannten Daten werden nicht an Dritte weitergegeben und von der revosec lediglich für den Zweck der genannten Services sowie für den Support verwendet.

Die revobox aktualisiert die Software-Version automatisch. Jede Nacht und beim Systemstart wird nach aktualiserten Software-Versionen gesucht und diese allenfalls automatisch installiert.

Lizenz- und Urheberrechts-Informationen

Die revobox enthält Open-Source Software. Der Quellcode von Software unter der *General Public License* sowie unter der *Lesser General Public License* ist Online[3] verfügbar. Diese Lizenzen geben Ihnen weitere Rechte an der Software, wie etwa den Einblick in Softwarequellen sowie deren Veränderung. Details zu Lizenz-Versionen sind den entsprechenden Software-Quellen zu entnehmen. Aktualisierte Lizenz-Informationen sind auf der revobox im Reiter *Gerät* verfügbar.

3 Open-Source Software-Quellen: http://master.revosec.net/sources

revosec AG
Bungerstrasse 5
CH-7323 Wangs

Tel. 081 284 53 82
support@revosec.ch
www.revosec.ch