

SSL-VPN NetExtender

Felizitas Heinebrodt

Georg-Simon-Ohm-Hochschule Nürnberg
Rechenzentrum
Kesslerplatz 12, 90489 Nürnberg

Version 5

Mai 2011

SSL-VPN NetExtender

Inhalt

- 1 Der NetExtender..... 1
- 2 Benötigte Zugangsdaten 1
 - 2.1 SSL-VPN-Gateway..... 1
 - 2.2 Domain, Username und Passwort..... 1
 - 2.2.1. Mit Ihrer my.ohm-Benutzerkennung 2
 - 2.2.2. Mit Ihrer VPN-Kennung 2
- 3 Das Virtual Office der Hochschule..... 2
 - 3.1 Authentifizierung..... 2
 - 3.2 Installation des NetExtender..... 2
 - 3.3 Automatische Updates 3
- 4 Direkt-Installation..... 3
 - 4.1 Automatische Updates 3
- 5 Aktivierung..... 3
- 6 Beenden der Sitzung..... 4
- 7 Noch Fragen???. 4

Als SSL-VPN bezeichnet man Systeme, die den Transport privater Daten über öffentliche Netzwerke ermöglichen (siehe VPN) und als Verschlüsselungsprotokoll TLS (alte Bezeichnung: SSL) verwenden.

An der OHM-Hochschule sorgt eine spezielle Hardware-Komponente, das **SSL-VPN-Gateway** für einen sicheren Zugang zum Hochschulnetz.

Um diesen Zugang nutzen zu können, müssen Sie einmalig eine Software, den NetExtender, installieren.

1 Der NetExtender

Der NetExtender baut eine sichere (verschlüsselte) Netzwerkverbindung über das Gateway auf und erlaubt Ihnen den Zugriff auf Ressourcen im Hochschulnetz, als ob Sie sich im lokalen Netz der Hochschule befinden würden.

Sie haben zwei Möglichkeiten, um den NetExtender auf Ihrem PC zu installieren.

- **Virtual Office**

Das SSL-VPN-Gateway unserer Hochschule verfügt über eine eigene Web-Oberfläche, das Virtual Office. Von dort aus können Sie eine Software, den NetExtender auf Ihrem PC/Mobilgerät installieren.

- **Direkt-Installation**

Auf der Webseite des Rechenzentrums finden Sie einen Link, von dem Sie die Installationssoftware – abhängig von Ihrem verwendeten Betriebssystem - direkt herunterladen und installieren können.

2 Benötigte Zugangsdaten

Unabhängig davon, wie Sie den NetExtender installieren, benötigen Sie folgende Angaben:

2.1 SSL-VPN-Gateway

Die Hochschule verfügt genau genommen über zwei SSL-VPN-Gateways. Die Beiden sind von der Funktion und Nutzung her völlig gleichwertig. Der Ausbau des SSL-VPN-Zugangs mit zwei Gateways soll zum Einen die Last verteilen und zum Anderen Ausfallsicherheit gewährleisten.

Die Adressen der SSL-VPN-Gateways sind
 vpnss11.cs.fh-nuernberg.de
 und
 vpnss12.cs.fh-nuernberg.de

Für Sie ist es egal, welche Adresse Sie hier angeben. Funktioniert allerdings der von Ihnen gewählte Zugang recht langsam, kann es unter Umständen helfen, die andere Adresse zu wählen.

2.2 Domain, Username und Passwort

Username und Passwort hängen davon ab, welche Domain Sie wählen.

Domain	Username + Passwort
my.OHM	my.OHM
radius.OHM	VPN-Konzentrator
ads1.OHM	Domäne ads1

Für den eigentlichen VPN-Tunnel spielt es später keine Rolle, welche Domain (bzw. welche Zugangsdaten) Sie hier nutzen.

2.2.1. Mit Ihrer my.ohm-Benutzerkennung

Sie wählen als Domain my.ohm.

Dann geben Sie in den Feldern darüber Ihren Benutzernamen und Ihr Passwort für my.ohm ein (die Kennung, mit der Sie zum Beispiel Ihre E-Mails abrufen).

Username: Ihr Benutzernamen für my.ohm

Passwort: Das dazugehörige my.ohm-Passwort

Domain: my.OHM

2.2.2. Mit Ihrer VPN-Kennung

Alternativ können Sie die Kennung benutzen, mit der Sie sich bisher am VPN angemeldet haben.

Dazu geben Sie als Domain radius.OHM ein und tragen in die Felder darüber Ihre VPN-Kennung ein.

Username: Ihr Benutzernamen für VPN (ist identisch mit Ihrem my.ohm-Benutzernamen)

Passwort: Das dazugehörige VPN-Passwort (stimmt nicht mit Ihrem my.ohm-Passwort überein, da zwischen diesen Systemen kein Abgleich stattfindet).

Domain: radius.OHM

3 Das Virtual Office der Hochschule

3.1 Authentifizierung

Zunächst bauen Sie in Ihrem Internet Browser eine Verbindung zu der Login-Seite des SSL-VPN-Gateways auf.

Dazu folgen Sie dem Link:

<https://vpnssl1.cs.fh-nuernberg.de/>

bzw.

<https://vpnssl2.cs.fh-nuernberg.de/>

Tipp: Es spielt für die Nutzung keine Rolle, welche der beiden Adressen Sie hier verwenden. Erscheint Ihnen ein Zugang zu langsam (möglicherweise wird er gerade besonders stark genutzt), wählen Sie einfach den anderen Zugang.

Sie werden nach Ihrer Benutzerkennung gefragt (siehe [Kapitel Zugangsdaten](#)).

Jetzt kommen Sie in das Virtual Office der Hochschule, die SSL-VPN-Portalseite.

Hier stehen Ihnen verschiedene Bookmarks zur Verfügung. Bei der Nutzung dieser Bookmarks arbeitet das Gateway als **HTTPS – Proxy**.

3.2 Installation des NetExtender

Sie klicken im Virtual Office auf

➤ [Click to Connect](#)



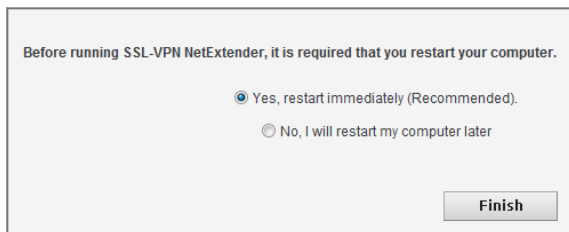
Möglicherweise erscheint am oberen Rand Ihres Browserfensters die Aufforderung, ActiveX zu installieren. Sie klicken auf

- [Install ActiveX Control](#)

Außerdem erhalten Sie vielleicht einen Warnhinweis von Windows. Sie klicken auf

- [Treibersoftware trotzdem installieren](#)

Danach startet die Installation.



Jetzt müssen Sie Ihren PC neu starten.

3.3 Automatische Updates

Installieren Sie den NetExtender über das Virtual Office, lädt er selbstständig Updates herunter, wenn sich auf dem SSL-VPN eine neue Version befindet.

4 Direkt-Installation

Zunächst laden Sie die Software auf Ihren PC herunter. Die Links für den Download finden Sie auf den Webseiten des Rechenzentrums. Sie benötigen Ihre my.ohm-Benutzerkennung.

Tipp: Für die Installation müssen Sie an Ihrem PC als Administrator angemeldet sein.

Sie folgen den Anweisungen der Installation.



Beim ersten Start des NetExtender benötigen Sie verschiedene Angaben

(siehe [Kapitel Zugangsdaten](#)).



4.1 Automatische Updates

Entscheiden Sie sich für die Direktinstallation und installieren den NetExtender selbst, führt er keine automatischen Updates durch!

Haben Sie den NetExtender bereits per Direktinstallation eingerichtet und möchten automatische Updates haben, müssen sie den NetExtender deinstallieren und über den "Virtual Office" neu installieren. Das Rechenzentrum empfiehlt, hierfür den Internet Explorer zu verwenden.

5 Aktivierung

Ab sofort können Sie mit dem NetExtender eine sichere Verbindung aufbauen.

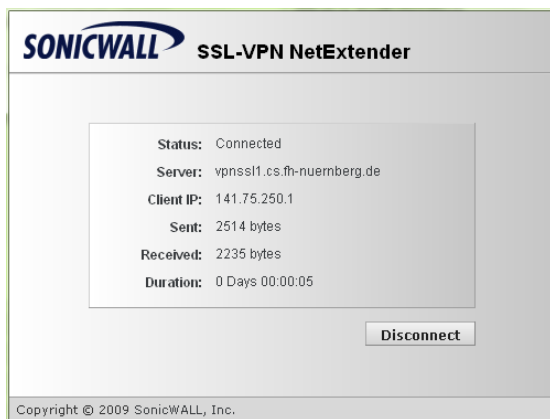
Dazu klicken Sie in Ihrer Taskleiste rechts unten mit der rechten Maustaste auf das Symbol des NetExtender



und wählen

➤ Connect

Tip: Sie können sich auch im Virtual Office anmelden und dann durch einen einfachen Mausklick auf NetExtender eine Verbindung aufbauen.



6 Beenden der Sitzung

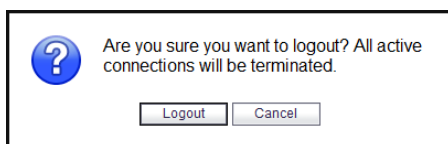
Um die SSL-VPN-Sitzung zu beenden, klicken Sie entweder im Virtual-Office rechts oben auf

➤ Logout



oder im Extender-Fenster auf

➤ Disconnect



7 Noch Fragen???

Ausführliche Hilfetexte (in englischer Sprache) finden Sie im Virtual Office rechts oben unter

➤ Help

