SOPHIA Protector

Benutzerhandbuch

Protector Software-Release 2.1

SOPHIA (Schweiz) AG
Morgenstrasse 131b
CH-3018 Bern
Telefon +41 31 994 1138
Fax +41 31 994 1128
info@sophia.ch
http://www.sophiafirewall.ch

November 2004

Inhalt

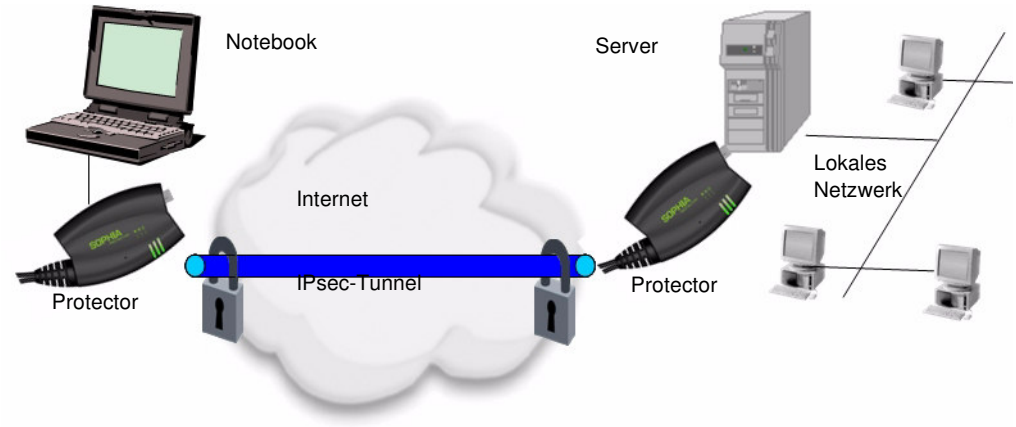
Inhalt

1 Einleitung

Der Protector sichert IP-Datenverbindungen. Dazu vereinigt das Gerät folgende Funktionen:

- VPN-Router (VPN - **V**irtuelles **P**rivates **N**etzwerk) für sichere Datenübertragung über öffentliche Netze (hardwarebasierte DES, 3DES und AES Verschlüsselung, IPsec Protokoll)
- Konfigurierbare Firewall für den Schutz vor unberechtigtem Zugriff. Der dynamische Paketfilter untersucht Datenpakete anhand der Ursprungs- und Zieladresse und blockiert unerwünschten Datenverkehr.
- Kaspersky-Virenschutz mit Unterstützung für die Protokolle HTTP, SMTP und POP3

Die Konfiguration des Gerätes erfolgt einfach mit einem Web-Browser.



VPN-Features

- Protokoll: IPsec (Tunnel und Transport Mode)
- IPsec DES Verschlüsselung mit 56 Bit
- IPsec 3DES Verschlüsselung mit 168 Bit
- IPsec AES Verschlüsselung mit 128, 192 und 256 Bit
- Paket-Authentifizierung: MD5, SHA-1
- Internet Key Exchange (IKE) mit Main und Quick Mode
- Authentisierung: Pre-Shared Key (PSK), X.509v3 Zertifikate
- DynDNS
- NAT-T
- Dead Peer Detection (DPD)

Firewall-Features

- Stateful Packet Inspection
- Anti-Spoofing
- NAT (IP Masquerading)
- Port Forwarding

Weitere Features

- DNS Cache
- DHCP Server
- Kaspersky-Virenschutz

Drei Geräteversionen

Der Protector wird in 3 Versionen ausgeliefert:

Protector S	Protector M	Protector L
• Stealth Firewall (ein Benutzer) • Router mit Anbindung über weitere Router, PPPoE oder PPTP • Konfigurierbare Firewall • Bis zu 2 IPsec VPN Verbindungen (erweiterbar) • Hardware Verschlüsselung (IPsec)	Wie Protector S, zusätzlich: • Bis zu 10 IPsec VPN Verbindungen (erweiterbar) • IPsec/L2TP Support • SNMP • Remote Logging	Wie Protector M, zusätzlich: • Bis zu 250 IPsec VPN Verbindungen (erweiterbar) • inkl. Netzteil

Support

Bei Problemen mit Ihrem Protector wenden Sie sich bitte an Ihren Händler. Zusätzliche Informationen zum Gerät, sowie Release Notes und Software-Updates finden Sie unter folgender Internet-Adresse: www.sophiafirewall.ch

2 Typische Anwendungsszenarien

Nachfolgend werden häufige und typische Anwendungsszenarien skizziert. Allen Szenarien ist gemeinsam, dass der Protector eine VPN-Verbindung über ein öffentliches Netz wie das Internet herstellt.
Der Protector und gegebenenfalls auch der/die angeschlossene(n) Client-Rechner muss/müssen gemäß des Anwendungs-Szenarios konfiguriert werden.

Szenario 1: Stealth

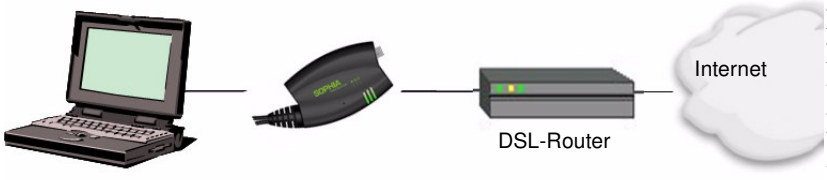
Gegenstelle:
Einzelrechner oder Netz/Subnetz mit vorgeschaltetem Router mit Firewall, z. B. ein anderer Protector

Netzwerk-Modus des Protector:

Stealth (Werkseinstellung) oder *Router*

Im Stealth-Modus ist beim lokal angeschlossenen Rechner keine Veränderung der bestehenden TCP/IP-Konfiguration erforderlich.

Szenario 2: Router



Gegenstelle:
wie oben:
Einzelrechner oder Netz/Subnetz mit vorgeschaltetem Router mit Firewall, z. B. ein anderer Protector

Netzwerk-Modus des Protector:

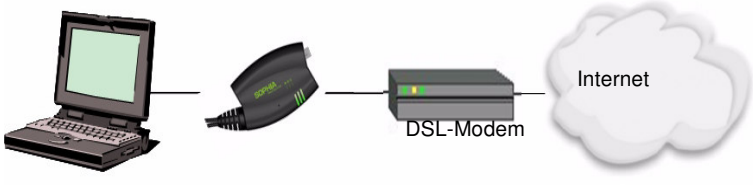
Router

Im *Router*-Modus muss beim lokal angeschlossenen Client-Rechner der Protector als Standardgateway festgelegt sein.

Beim NAT-Router ist keine weitere Konfiguration erforderlich auf Grund der NAT-T-Funktionalität des Protector.

Falls der Router eine Firewall hat, darf diese Port 500/udp und Port 4500/udp nicht sperren.

Szenario 3: PPPoE



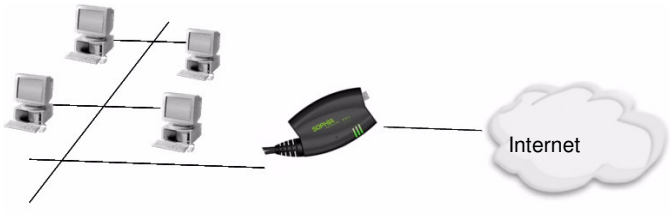
Gegenstelle:
wie oben:
Einzelrechner oder Netz/Subnetz mit vorgeschaltetem Router mit Firewall, z. B. ein anderer Protector

Netzwerk-Modus des Protector:

PPPoE

Im *PPPoE*-Modus muss beim lokal angeschlossenen Client-Rechner der Protector als Standardgateway festgelegt sein.

Szenario 4: Netzwerk-Router



Gegenstelle:
wie oben: Einzelrechner oder Netz/Subnetz mit vorgeschaltetem Router mit Firewall, z. B. ein anderer Protector

Netzwerk-Modus des Protector:

Router oder *PPPoE* oder *PPTP*

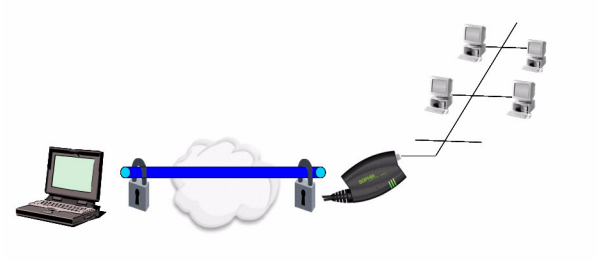
Router, wenn der Internet-Anschluss per Standleitung erfolgt

PPPoE, wenn der Internet-Anschluss z. B. per DSL-Modem erfolgt und dass das PPPoE-Protokoll verwendet wird (z. B. in Deutschland).

PPTP, wenn der Internet-Anschluss z. B. per DSL-Modem erfolgt, so dass das PPTP-Protokoll verwendet wird (z. B. in Österreich).

Bei dem/den lokal angeschlossenen Client-Rechner(n) muss der Protector als Standardgateway festgelegt sein.

Szenario 5: VPN



Auf dem Einzelrechner muss eine extra VPN-Client Software ausgeführt werden. Erhältlich beim SOPHIA Support. Unter Windows 2000 oder höher kann die in das Betriebssystem integrierte VPN-Funktion integriert werden.

2.1 DynDNS-Service

Der Aufbau einer VPN-Verbindung zwischen zwei Standorten wird vorausgesetzt, dass die IP-Adresse von mindestens einem Standort bekannt und damit definierbar ist. Bei vielen Internet Service Providern (ISPs) werden die IP-Adressen jedoch dynamisch zugewiesen, d. h. die IP-Adressen der Rechner bzw. Netze, die Zugriff zum Internet haben, ändern sich.

Um die Problematik der dynamischen IP-Adressenvergabe zu lösen, können sog. DynDNS-Dienste genutzt werden. Durch einen solchen Dienst ist der Protector immer über einen festen Domain Namen zu erreichen, unabhängig von der aktuellen IP-Adresse. Bei jedem Wechsel der IP-Adresse meldet der Protector die neue IP-Adresse dem DynDNS Server, so dass auf dem DNS-Server dem Domain Namen stets die aktuelle IP-Adresse zugeordnet ist - siehe Glossar.

Die Nutzung eines DynDNS-Dienstes erfordert den Abschluss eines Vertrages mit dem entsprechenden Anbieter, z. B. DynDNS.org oder DNS4BIZ.com.

3 Bedienelemente und Anzeigen

LEDs	Farbe	Zustand	Bedeutung
2	Rot/Grün	rot-grün blinkend	**Bootvorgang**. Nach Anschluss des Gerätes an die Stromversorgungsquelle. Nach einigen Sekunden wechselt diese Anzeige zu Heartbeat.
	Grün	blinkend	**Heartbeat**. Das Gerät ist korrekt angeschlossen und funktioniert.
	Rot	blinkend	**Systemfehler**. ⌧ Führen Sie einen Neustart durch. Dazu die Recovery-Taste kurz (1,5 Sek.) drücken ODER Das Gerät von der Stromversorgung kurz trennen und dann wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die *Recovery-Prozedur* (siehe „Recovery-Prozedur ausführen” auf Seite 79) oder wenden Sie sich an den Support.
1 und **3**	Grün	leuchtend oder blinkend	**Ethernetstatus**. LED 1 zeigt den Status des internen Interface, LED 3 den Status des externen. Sobald das Gerät am externen Netzwerk (WAN, Internet) angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner besteht. Bei der Übertragung von Datenpaketen erlischt kurzzeitig die LED.
1, 2, 3	div. LED-Leuchtcodes		**Recovery-Modus**. Nach Drücken der **Recovery**-Taste. Siehe „Die Recovery-Taste für Neustart, Recovery-Prozedur und Flashen der Firmware” auf Seite 79.

4 Inbetriebnahme

Sicherheits-hinweise

Der SOPHIA Protector ist für den Betrieb bei Schutzkleinspannung vorgesehen. Schließen Sie die Netzwerkinterfaces des Protector nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen. Der Protector darf nicht an Fernmeldeanschlüssen betrieben werden.

Warnung! Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Massnahmen durchzuführen.

Allgemeine Hinweise zur Benutzung

- Zum Reinigen des Gerätegehäuses ein weiches Tuch verwenden. Kein aggressives Lösungsmittel auftragen!
- Umgebungsbedingungen:
  0 bis +40° Celsius,
  max. Luftfeuchtigkeit 90%, nicht kondensierend
- Nicht direktem Sonnenlicht oder dem Einfluss einer Wärmequelle aussetzen, um Überhitzung zu vermeiden.
- Anschlusskabel nicht knicken. Den Netzwerkstecker nur zum Verbinden mit einem Netzwerk benutzen.

Schritte zur Inbetriebnahme

Um das Gerät in Betrieb zu nehmen, führen Sie folgende Schritte in der angegebenen Reihenfolge aus:

Schritt	Ziel	Seite
1	Lieferumfang prüfen, Release Notes lesen	Lieferumfang
2	Gerät anschließen	Gerät anschließen
3	Das Gerät konfigurieren, soweit erforderlich. Gehen Sie dazu die einzelnen Menüoptionen durch, die Ihnen der Protector mit seiner Konfigurationsoberfläche bietet. Lesen Sie deren Erläuterungen in diesem Handbuch, um zu entscheiden, welche Optionen mit welcher Einstellung für Ihre Betriebsumgebung erforderlich oder gewünscht wird.	Lokale Konfiguration: Bei Inbetriebnahme

4.1 Lieferumfang

Prüfen Sie vor Inbetriebnahme die Lieferung auf Vollständigkeit:

Zum Lieferumfang gehören

- Das Gerät Protector S, M oder L
- Ein Netzteil (nur bei Protector L)
- Handbuch im .pdf-Format auf CD
- Quick Installation Guide

4.2 Gerät anschließen

USB-Stecker zum Anschließen an die USB-Schnittstelle eines Rechners.
Dient nur zur Stromversorgung!

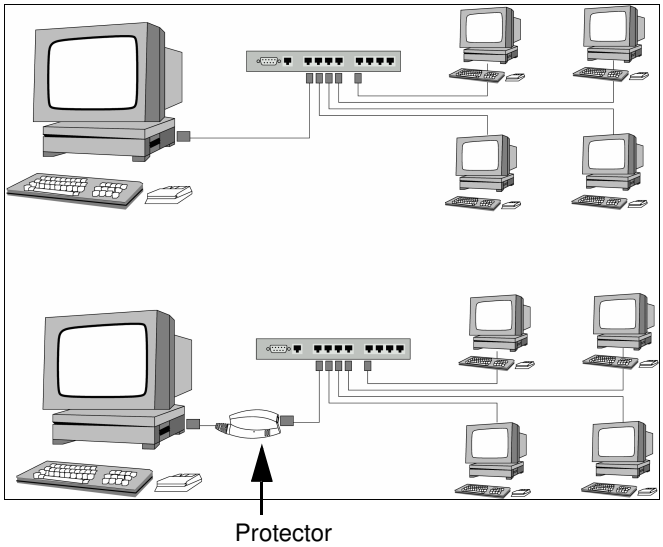
Ethernet-Stecker zum direkten Anschließen an das zu schützende Gerät bzw. Netz (**lokales** Gerät oder Netz).

Buchse zum Anschließen an das externe Netzwerk, z. B. WAN, Internet.
(Über dieses Netz werden die Verbindungen zum entfernten Gerät bzw. Netz hergestellt.)
Benutzen Sie ein UTP-Kabel (CAT 5).

Wenn Ihr Rechner bereits an einem Netzwerk angeschlossen ist, dann stekken Sie den Protector zwischen Netzwerk-Interface des Rechners und Netzwerk.

vorher:

nachher:



⌦ Es ist keine Treiber-Installation erforderlich.

⌦ Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administratorpasswort zu ändern.

5 Konfiguration

Voraussetzungen

- Bei lokaler Konfiguration: Der Rechner, mit dem Sie die Konfiguration vornehmen, muss entweder
  – am Ethernet-Stecker des Protector angeschlossen sein,
  – oder er muss über das lokale Netzerk mit ihm verbunden sein.
- Bei Fernkonfiguration: Der Protector muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der Protector muss eingeschaltet sein, d. h. per USB-Kabel an einen eingeschalteten Rechner (oder Netzteil) angeschlossen sein, so dass er mit Strom versorgt wird.
- Der Protector muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

5.1 Lokale Konfiguration: Bei Inbetriebnahme

Der Protector wird per Web-Browser konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird (z. B. MS Internet-Explorer ab Version 5.0 oder Netscape Communicator ab Version 4.0)

⌧Der Web-Browser muss SSL (d. h. https) unterstützen.

Der Protector ist gemäß Werkseinstellung unter folgender Adressen erreichbar:

Werkseinstellung:

Stealth-Modus (Auslieferungszustand): https://1.1.1.1/

Bei konfigurierter Netzwerk-Schnittstelle

Damit der Protector über die Adresse https://1.1.1.1/ angesprochen werden kann, muss er an eine konfigurierte Netzwerk-Schnittstelle angeschlossen sein. Das ist der Fall, wenn man ihn zwischen eine bestehende Netzwerkverbindung steckt - siehe Abbildung im Abschnitt „Gerät anschließen” auf Seite 10.

In diesem Fall wird der Web-Browser nach Eingabe der Adresse https://1.1.1.1/ die Verbindung zur Konfigurations-Oberfläche des Protector herstellen - siehe „Lokale Konfigurationsverbindung herstellen” auf Seite 13. Fahren Sie in diesem Falle dort fort.

Bei nicht konfigurierter Netzwerk-Schnittstelle

Falls die Netzwerk-Schnittstelle des Rechners nicht konfiguriert ist...

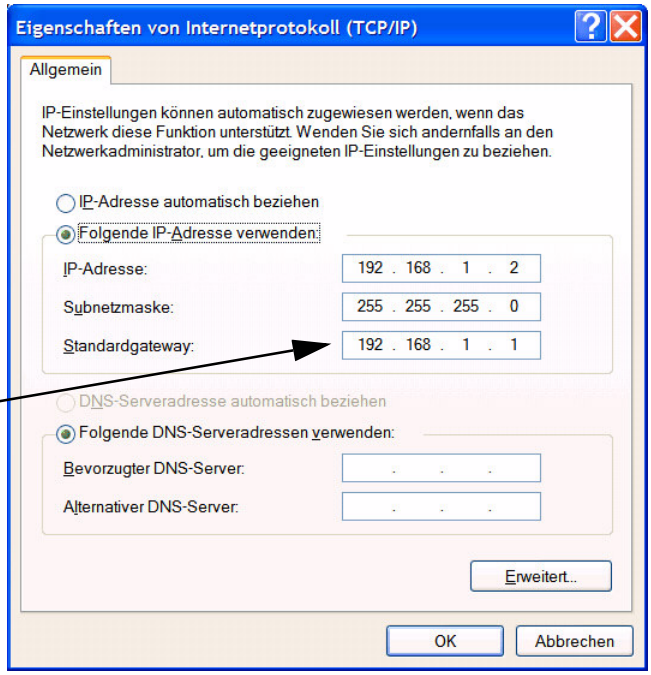
Wenn der Konfigurations-Rechner noch nicht an einem Netzwerk angeschlossen war, z. B. weil der Rechner neu ist, dann ist seine Netzwerk-Schnittstelle im Allgemeinen nicht konfiguriert. Das heißt der Rechner „weiß“ noch nicht, dass der Netzwerkverkehr über diese Schnittstelle läuft.

In diesem Fall müssen Sie den Standardgateway initialisieren, indem Sie ihm einen Dummy-Wert zuweisen. Gehen Sie dazu wie folgt vor:

Standardgateway initialisieren

1. Ermitteln Sie die zurzeit gültige Standardgateway-Adresse.
   Unter Windows XP klicken Sie dazu **Start, Systemsteuerung, Netzwerkverbindungen**: Symbol des LAN-Adapters mit der rechten Maustaste klikken und im Kontextmenü **Eigenschaften** klicken. Im Dialogfeld *Eigenschaften von LAN-Verbindung lokales Netz* auf der Registerkarte *Allgemein* unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag

Internetprotokoll (TCP/IP) markieren und dann die Schaltfläche **Eigenschaften** klicken, so dass folgendes Dialogfeld angezeigt wird:



Hier die IP-Adresse des Standardgateway nachschlagen oder festlegen.

Falls in diesem Dialogfeld keine IP-Adresse des Standardgateway angegeben ist, z. B. weil *IP-Adresse automatisch beziehen* aktiviert ist, dann geben Sie eine IP-Adressen manuell ein. Dazu aktivieren Sie zunächst **Folgende IP-Adressen verwenden** und geben dann zum Beispiel folgende Adressen ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standardgateway:	192.168.1.1

⌦ Auf keinen Fall dem Konfigurations-Rechner eine Adresse wie 1.1.1.2 geben!

2. Auf DOS-Ebene (Menü **Start, Alle Programme, Zubehör, Eingabeaufforderung**) geben Sie ein:
   `arp -s` <IP des Standardgateway> **`aa-aa-aa-aa-aa-aa`**
   Beispiel:
   Sie haben als Standardgateway-Adresse ermittelt oder festgelegt: 192.168.1.1
   Dann lautet der Befehl:
   `arp -s 192.168.1.1 aa-aa-aa-aa-aa-aa`

3. Zur Konfiguration stellen Sie jetzt die Konfigurationsverbindung her - siehe „Lokale Konfigurationsverbindung herstellen” auf Seite 13

4. Nach der Konfiguration stellen Sie das Standardgateway wieder zurück. Dazu entweder den Konfigurations-Rechner neu starten oder auf DOS-Ebene folgendes Kommando eingeben:
   `arp -d`

⌦ Je nach dem, wie Sie den Protector konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.

5.2 Lokale Konfigurationsverbindung herstellen

Web-basierte Administrator-oberfläche

Der Protector wird per Web-Browser konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird (z. B. MS Internet-Explorer ab Version 5.0 oder Netscape Communicator ab Version 4.0)

⌦Der Web-Browser muss SSL (d. h. https) unterstützen.

Je nach dem, in welchem Netzwerk-Modus (= Betriebsart) der Protector sich befindet, ist er gemäß Werkseinstellung unter einer der folgenden Adressen erreichbar:

Werkseinstellung:

Stealth-Modus (Auslieferungszustand):	https://1.1.1.1/
Router- / PPPoE- / PPPT-Modus:	https://192.168.1.1/

Gehen Sie wie folgt vor:

1. Starten Sie einen Web-Browser.
   (Z. B. MS Internet-Explorer ab Version 5.0 oder Netscape Communicator ab Version 4.0; der Web-Browser muss SSL (d. h. https) unterstützen.)
2. Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt, weil sonst sonst die Verbindungsaufnahme zum Protector erschwert werden könnte.
   Im MS Internet Explorer nehmen Sie diese Einstellung wie folgt vor: Menü **Extras, Internetoptionen...**, Registerkarte *Verbindungen*:
   Unter *DFÜ- und VPN-Einstellungen* muss **Keine Verbindung wählen** aktiviert sein.
3. In der Adresszeile des Web-Browsers geben Sie die Adresse des Protector vollständig ein.

IP-Adresse des Protector im *Stealth*-Modus:
https://1.1.1.1/

Im **Stealth**-Modus (= Werkseinstellung) lautet diese fest:
`https://1.1.1.1/`

im Router- oder PPPoE-Modus:
https://192.168.1.1/

Sollte das Gerät schon einmal konfiguriert worden sein und dabei auf die Betriebsart **Router**, **PPPoE** oder **PPTP** gestellt worden sein, dann lautet die Adresse des Protector gemäß Werkseinstellung:
`https://192.168.1.1/`

↓

Folge:
Sie gelangen zur Administrator-Website des Protector. Der auf der nächsten Seite abgebildete Sicherheitshinweis erscheint.

⌦Falls Sie die konfigurierte Adresse vergessen haben:

Falls die Adresse des Protector im *Router- PPPoE-* oder *PPTP*-Modus auf einen anderen Wert gesetzt ist und Sie kennen die aktuelle Adresse nicht, dann müssen Sie den Protector mit Hilfe der **Recovery**-Taste zurück auf den Stealth-Modus stellen und damit auf folgende Adresse: https://1.1.1.1/ (siehe „Recovery-Prozedur ausführen” auf Seite 79).

⌦Falls die Administrator-Website nicht angezeigt wird...

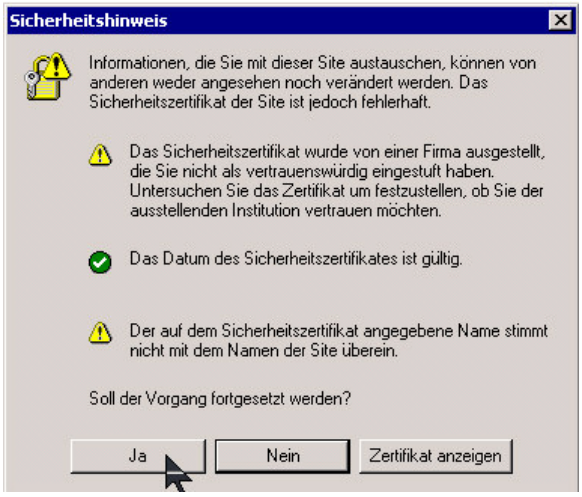
Sollte auch nach wiederholtem Versuch der Web-Browser melden, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Prüfen Sie, ob der Standardgateway des angeschlossenen Konfigurations-Rechners initialisiert ist. Siehe „Lokale Konfiguration: Bei Inbetriebnahme” auf Seite 11
- Eine bestehende Firewall gegebenenfalls deaktivieren.

- Achten Sie darauf, dass der Browser keinen Proxy Server verwendet.
  Im MS Internet Explorer (Version 6.0) nehmen Sie diese Einstellung wie folgt vor: Menü **Extras, Internetoptionen...**, Registerkarte *Verbindungen*: Unter *LAN-Einstellungen* auf die Schaltfläche **Einstellungen...** klicken, im Dialogfeld *Einstellungen für lokales Netzwerk (LAN)* dafür sorgen, dass unter Proxyserver der Eintrag **Proxyserver für LAN verwenden** nicht aktiviert ist.
- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.
  Unter Windows Menü **Start, Einstellungen, Systemsteuerung, Netzwerkverbindungen** bzw. **Netzwerk- und DFÜ-Verbindungen** das betreffende Symbol mit der rechten Maustaste klicken und im Kontextmenü **Deaktivieren** wählen.

Bei erfolgreichem Verbindungsaufbau

Nach erfolgreicher Verbindungsaufnahme erscheint dieser Sicherheitshinweis (MS Internet-Explorer):



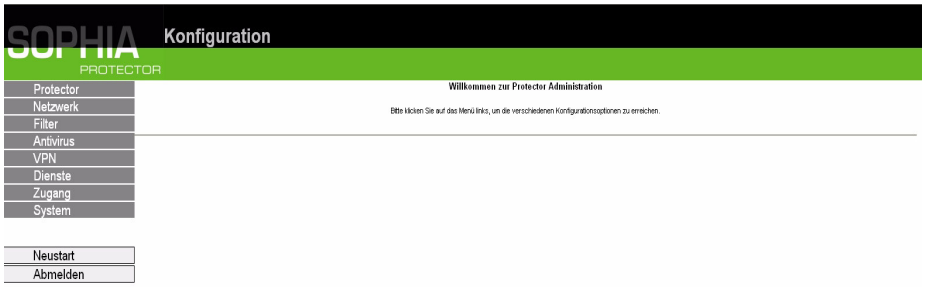
Erläuterung:
Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbstunterzeichneten Zertifikat ausgeliefert.

Quittieren Sie den entsprechenden Sicherheitshinweis mit **Ja**.

Folge:
Nach Abfrage des Benutzernamens (Login) und Passwortes wird die Administrator-Website des Protector wird angezeigt.
Werksseitig sind folgende Accounts voreingestellt:

Login:	**`admin`**
Passwort:	**`Protector`**
Login:	**`root`**
Passwort:	**`root`**

⌦ Groß- und Kleinschreibung beachten!



Konfiguration durchführen

Zur Konfiguration gehen Sie wie folgt vor:

1. Per Menü die Seite mit den gewünschten Einstellmöglichkeiten aufrufen - siehe ab Seite 23.
2. Auf der betreffenden Seite die gewünschten Einträge machen
3. Mit **OK** ggf. bestätigen, so dass die Einstellungen vom Gerät übernommen werden.
   Gegebenenfalls erhalten Sie vom System eine (bestätigende) Rückmeldung.

Sollte bei erneuter Anzeige einer Seite diese nicht aktuell sein, weil der Browser sie aus dem Cache lädt, aktualisieren Sie die Anzeige der Seite. Dazu in der Browser-Symbolleiste das Symbol zum Aktualisieren klicken.

⌦ Je nach dem, wie Sie den Protector konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.

5.3 Fernkonfiguration

Voraussetzung

Der Protector muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.

⌦ Standardmäßig ist die Möglichkeit zur Fernkonfiguration ausgeschaltet.

Um die Möglichkeit zur Fernkonfiguration einzuschalten, siehe Abschnitt „Zugang → HTTPS" auf Seite 69.

Fernkonfiguration durchführen

Um von einem entfernten Rechner aus den Protector zu konfigurieren, stellen Sie von dort die Verbindung zum lokalen Protector her.
Gehen Sie wie folgt vor:

1. Starten Sie dazu auf dem entfernten Rechner den Web-Browser (z. B. MS Internet-Explorer ab Version 5.0 oder Netscape Communicator ab Version 4.0; der Web-Browser muss SSL (d. h. https) unterstützen.)
2. Als Adresse geben Sie an: Die IP-Adresse, unter der die Gegenstelle über das Internet bzw. WAN erreichbar ist, zusätzlich die Port-Nummer.

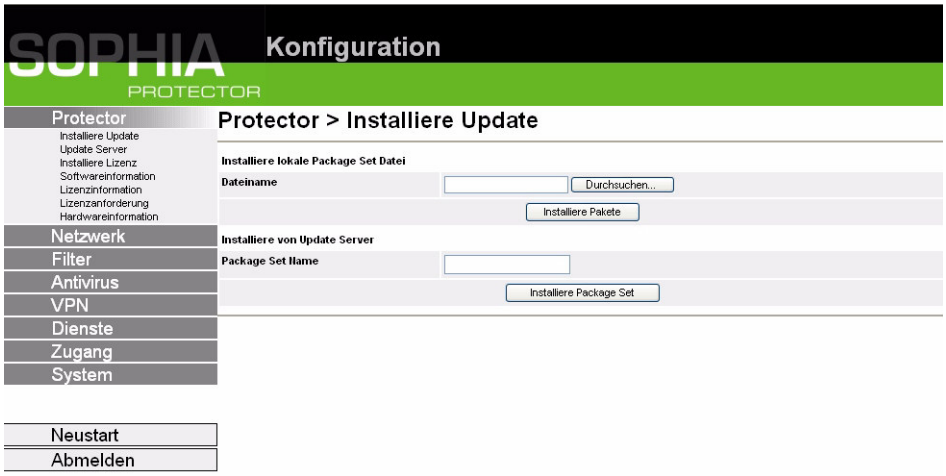
   Beispiel:
   Ist dieser Protector über die Adresse 192.144.112.5 über das Internet zu erreichen, und ist für den Fernzugang die Port-Nummer 443 festgelegt, dann muss bei der entfernten Gegenstelle im Web-Browser folgende Adresse angegeben werden: 192.144.112.5

Bei einer anderen Port-Nummer ist diese hinter der IP-Adresse anzugeben, z. B.: 192.144.112.5:442

⌦ Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administratorpasswort zu ändern - siehe „Zugang → Passworte" auf Seite 68.

5.4 Menü Protector

Protector → Installiere Update



Lesen Sie die README-Datei!

Voraussetzung: Sie haben ein aktuelles Software-Paket entweder
– lokal auf Ihrem Konfigurations-Rechner gespeichert haben
ODER
– über einen entfernten Server zur Verfügung gestellt bekommen.

⌦ Ob und auf welche Weise Sie an ein Software-Update gelangen können, erfragen Sie bei Ihrem Distributor.

⌦ **Sie dürfen während des Updates auf keinen Fall die Stromversorgung des Protector unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.**

Haben Sie ein aktuelles Software-Update auf Ihrem Konfigurations-Rechner gespeichert, gehen Sie wie folgt vor:

1. **Durchsuchen...** klicken und dann die Datei selektieren.
2. **Installiere Pakete** klicken, um sie in das Gerät zu laden.
   Dieser Vorgang kann je nach Größe des Updates mehrere Minuten dauern.

Sollte nach dem System-Update ein Reboot erforderlich sein, wird das angezeigt.

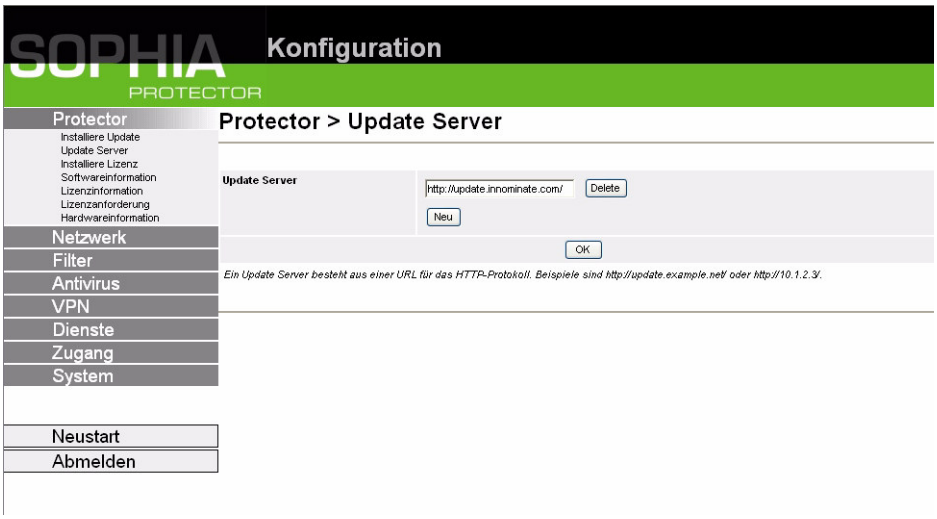
- Wird Ihnen ein aktuelles Software-Update auf einem entfernten Server zur Verfügung gestellt, muss dessen Adresse festgelegt sein - siehe „Protector → Update Server" auf Seite 18.

Gehen Sie wie folgt vor:

1. Schreiben Sie den Dateinamen in das Eingabefeld.
2. **Installiere Package Set** klicken, um sie in das Gerät zu laden.
   Dieser Vorgang kann je nach Größe des Updates mehrere Minuten dauern.

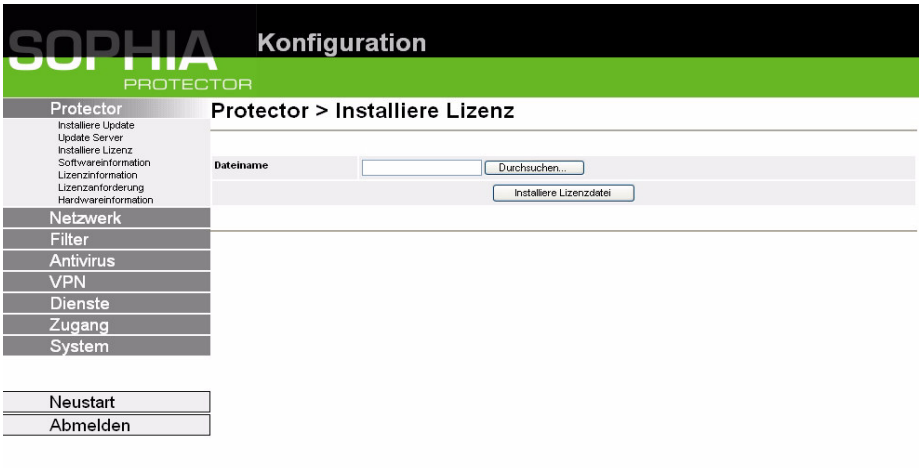
Sollte nach dem System-Update ein Reboot erforderlich sein, wird das angezeigt.

Protector → Update Server



Wird Ihnen ein Software-Update (siehe „Protector → Installiere Update" auf Seite 17) des Protector auf einem entfernten Server zur Verfügung gestellt, dann geben Sie hier dessen Adresse an. Dieser muss auf jeden Fall das benutzte Protokoll voranstehen.
Beispiele: http://123.456.789.1 oder http: //www.xyz.com/update

Protector → Installiere Lizenz

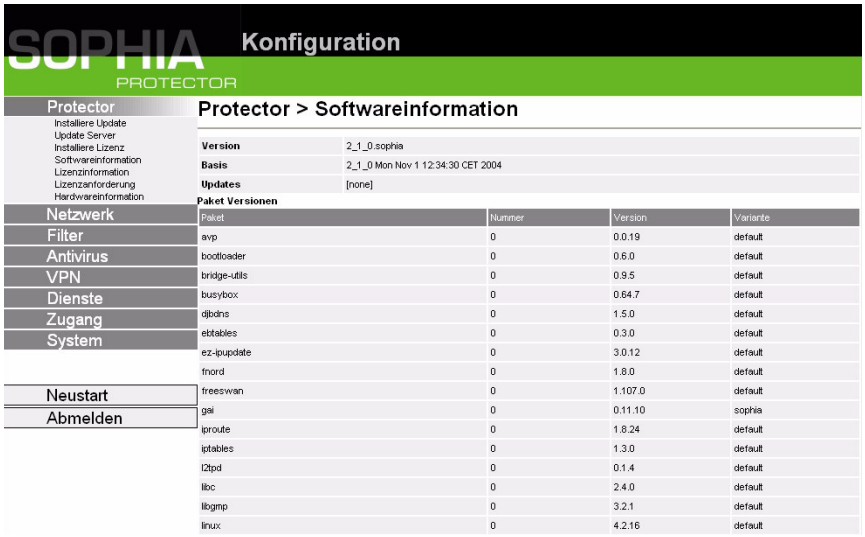


Voraussetzung: Sie haben von Ihrem Distributor eine Lizenzdatei für den Protector erworben und haben diese Datei auf dem Konfigurations-Rechner gespeichert.
Installieren Sie die Lizenzdatei wie folgt:

1. **Durchsuchen...** klicken und dann die Datei selektieren.
2. **Installiere Lizenzdatei** klicken, um sie in das Gerät zu laden.

Protector → Software-information

Nur Anzeige

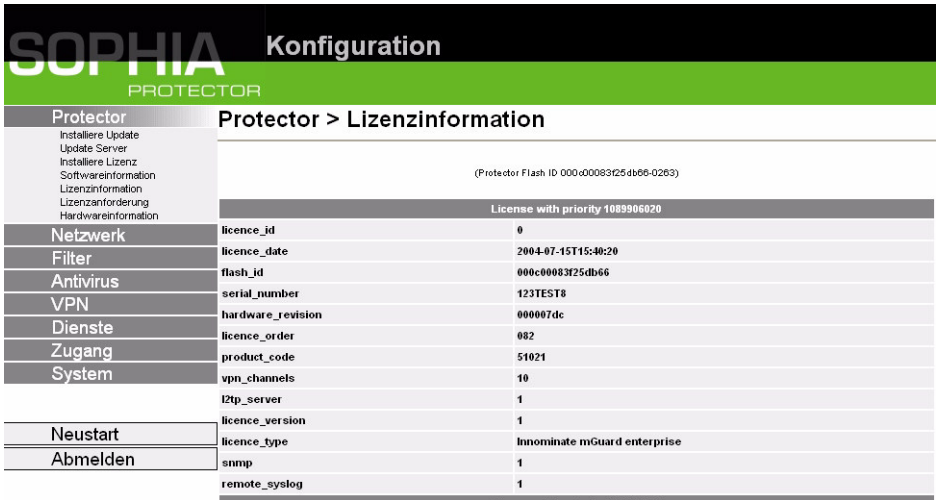


Listet die im Gerät befindlichen Software-Module auf. Diese werden als Pakete bezeichnet.

Dient für Update-Zwecke: Vergleichen Sie die angezeigten Versionsnummern mit den aktuellen Versionsnummern der entsprechenden Pakete. Bitte wenden Sie sich dazu an Ihren Distributor.
Falls neue Versionen verfügbar sind, können Sie die Software im Gerät updaten. Siehe „Protector → Installiere Update” auf Seite 17.

Protector → Lizenz-information

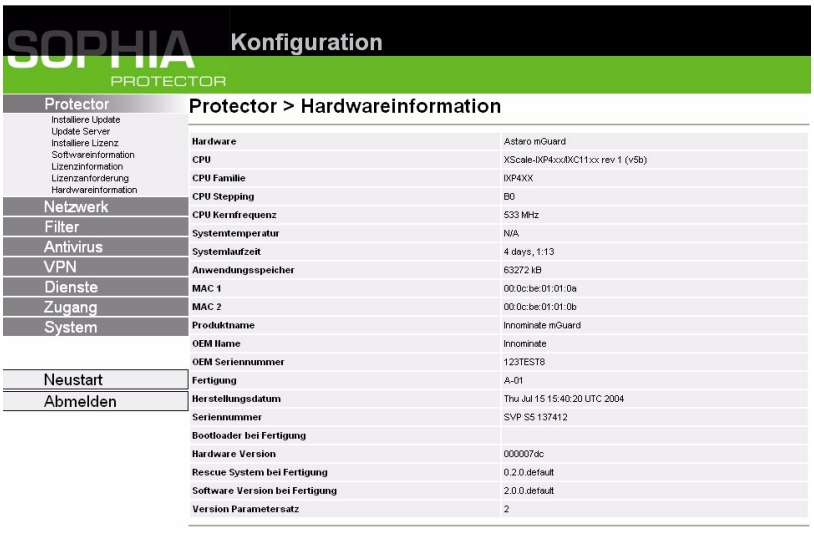
Nur Anzeige



Listet die erworbenen Lizenzen auf. Die entsprechenden Lizenzdateien sind im Protector installiert. Siehe „Protector → Installiere Lizenz” auf Seite 18.

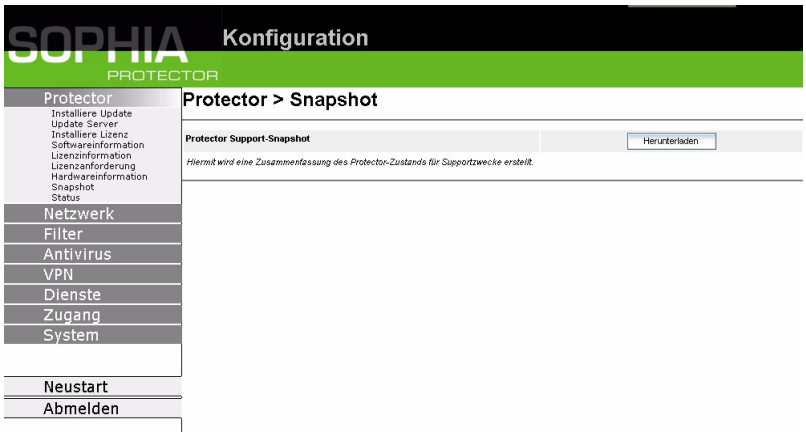
Protector → Hardware-information

Nur Anzeige



Für erfahrene Systemadministratoren / Support.

Protector → Snapshot



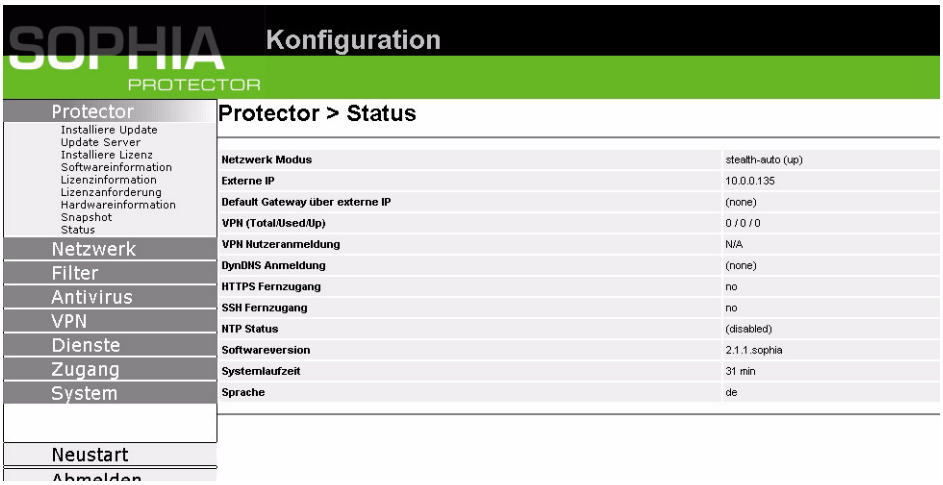
Diese Funktion dient für Support-Zwecke des SOPHIA Support.
Erstellt eine komprimierte Datei (im tar-Format), in der alle aktuellen Konfigurations-Einstellungen und Log-Einträge erfasst sind, die zur Fehlerdiagnose relevant sein könnten. (Diese Datei enthält keine privaten Informationen wie z. B. das private Machinen-Zertifikat oder die Passwörter. Eventuell benutzte Pre-Shared Keys von VPN-Verbindungen sind jedoch in den Snapshots enthalten.)
Um einen Snapshot zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie **Herunterladen**.
2. Speichern Sie die Datei unter dem Namen *snapshot.tar.gz*

Stellen Sie die Datei dem SOPHIA Support zur Verfügung, wenn dieser danach fragt.

Protector → Status

Nur Anzeige



Zeigt eine Zusammenfassung verschiedener Statusinformationen für Support-Zwecke:

Netzwerk-Modus: Betriebsart des Protector: *Stealth, Router*, *PPPoE* oder *PPTP*

Externe IP:

Die IP-Adresse des Protector an seinem Anschluss für das externe Netz (WAN bzw. Internet).
Im *Stealth*-Modus übernimmt der Protector die Adresse des lokal angeschlossenen Rechners für diese Schnittstelle.

Default Gateway über externe IP: Hier wird die externe IP-Adresse des Protector angezeigt. Im *Stealth*-Modus ist das gleich der IP-Adresse des Client.

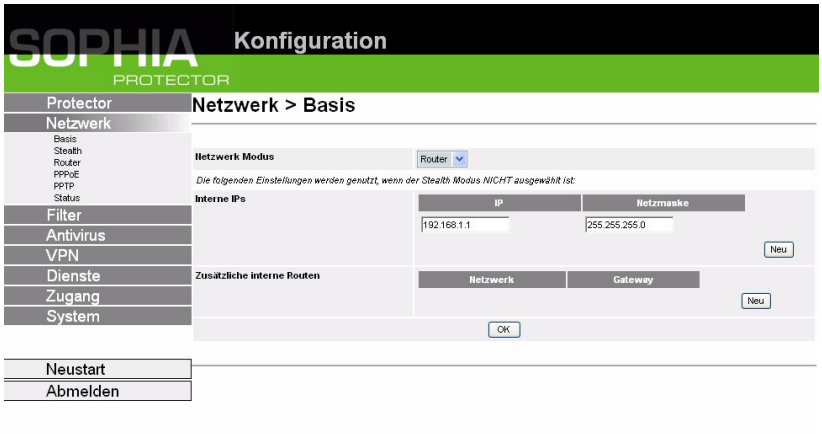
VPN (Total / Used / Up): Möglichkeiten: *Total / Used / Up*
Total: Insgesamt eingerichtete VPN-Verbindungen
Used: Benutzte VPN-Verbindungen
Up: Gegenwärtig aktive VPN-Verbindungen

VPN Nutzeranmeldung: Möglichkeiten:
N / A : Nicht verfügbar (not available)
not logged in : VPN gesperrt
logged in : VPN freigeschaltet

DynDNS Anmeldung:	Möglichkeiten: *none / Angabe des DynDNS-Server / failure / trying* *none*: Kein DynDNS-Server angegeben *Angabe des DynDNS-Server*: Adresse des DynDNS-Servers, den der Protector zur Auflösung von Hostnamen benutzt *failure*: Der Protector versucht vergeblich, eine Verbindung zum DynDNS-Server herzustellen. *trying*: Der Protector versucht gerade, eine Verbindung zum DynDNS-Server herzustellen.
HTTPS Fernzugang:	Möglichkeiten: *no / yes*
SSH Fernzugang:	Möglichkeiten: *no / yes*
NTP Status:	Möglichkeiten: *synchonized / not synchronized* *synchronized*: Über das Network Time Protokoll empfängt der Protector von einem Zeitserver die aktuelle Uhrzeit (Greenwich-Zeit). *not synchronized*: Der Protector ist mit keinem Zeitserver verbunden und kann deshalb nicht die aktuelle Uhrzeit liefern.
Softwareversion:	Version der im Protector installierten Software
Systemlaufzeit:	Laufzeit seit dem letzten Startvorgang des Protector.
Sprache:	Aktuell eingestellte Sprache

5.5 Menü Netzwerk

Netzwerk → Basis



Netzwerk Modus

Der Protector muss auf den Netzwerk-Modus (= Betriebsart) gestellt werden, der seiner lokalen Rechner- bzw. Netzwerk-Anbindung entspricht. Siehe „Typische Anwendungsszenarien" auf Seite 6.

⌦ Beim Wechsel des Netzwerk-Modus bootet das Gerät automatisch neu.

⌦ Wenn Sie die Adresse des Protector ändern (z. B. durch Wechsel des Netzwerk-Modus von *Stealth* auf *Router*), dann ist das Gerät ab sofort nach Neustart nur noch unter der neuen Adresse zu erreichen. Siehe „Lokale Konfiguration: Bei Inbetriebnahme" auf Seite 11.

⌦ Wenn Sie den Modus auf *Router* oder *PPPoE* oder *PPTP* stellen und dann die interne IP-Adresse und/oder die lokale Netzmaske ändern, achten Sie unbedingt darauf, dass Sie korrekte Werte angeben. Sonst ist der Protector nicht mehr erreichbar.

Transparenter Protector

Stealth (Werkseinstellung)

Der *Stealth*-Modus wird ausschließlich zur lokalen Anbindung eines einzelnen Computers als Client verwendet.

In dieser Betriebsart kann das Gerät einfach in eine bestehende Netzwerkanbindung des betreffenden Rechners integriert werden. Dazu einfach den Protector zwischenschalten - siehe Abbildung im Abschnitt „Gerät anschließen" auf Seite 10.

Der Protector analysiert den laufenden Netzwerkverkehr und konfiguriert dementsprechend seine Netzwerkanbindung eigenständig und arbeitet transparent, d. h. ohne dass der Client umkonfiguriert werden muss.

Wie auch in den anderen Modi stehen die Sicherheitsfunktionen Firewall und VPN zur Verfügung.

Von extern gelieferte DHCP-Daten werden an den angeschlossenen Client durchgelassen.

⌦ Ist **Stealth** als Netzwerk-Modus gewählt, sind keine Einträge zu machen unter *Interne IPs* und *Zusätzliche interne Routen*. Vorhandene Einträge unter diesen Punkten werden ignoriert.

Protector als Router

Router

Befindet sich der Protector nicht im *Stealth*-Modus, arbeitet er als normaler Router und hat dabei eine externe und eine interne IP-Adresse.

Der Protector ist über seine externe Schnittstelle per Ethernet-Standleitung ans Internet angeschlossen oder über weitere Router ans LAN.

An seine interne Schnittstelle ist ein Netzwerk oder ein Einzelrechner als Client angeschlossen. Der Protector fungiert für diesen bzw. dieses als Gateway. Wie auch in den anderen Modi stehen die Sicherheitsfunktionen Firewall und VPN zur Verfügung.

- Wird der Protector im *Router*-Modus betrieben, muss bei lokal angeschlossenen Client-Rechnern der Protector als Standardgateway festgelegt sein. D. h. die Adresse des Standardgateway ist auf die interne IP des Protector zu setzen. Siehe „☞ IP-Konfiguration bei Windows-Clients" auf Seite 65.
- Wird der Protector im *Router*-Modus betrieben und stellt die Verbindung zum Internet her, sollte NAT aktiviert werden, um aus dem lokalen Netz heraus Zugriff auf das Internet zu erhalten - siehe „Filter → NAT" auf Seite 33. Ist NAT nicht aktiviert, können nur VPN-Verbindungen genutzt werden.

Protector als Router

Der Protector arbeitet auch im PPPoE- oder PPTP-Modus als Router.

PPPoE

Der *PPPoE*-Modus entspricht dem Router-Modus mit DHCP - mit einem Unterschied: Für den Anschluss ans externe Netzwerk (Internet, WAN) wird - wie in Deutschland - das PPPoE-Protokoll verwendet, das von vielen DSL-Modems (bei DSL-Internetzugang) verwendet wird. Die externe IP-Adresse, unter der der Protector von einer entfernten Gegenstelle aus erreichbar ist, wird vom Provider dynamisch festgelegt.

- Wird der Protector im *PPPoE*-Modus betrieben, muss bei lokal angeschlossenen Client-Rechnern der Protector als Standardgateway festgelegt sein. D. h. die Adresse des Standardgateway ist auf die interne IP des Protector zu setzen. Siehe „☞ IP-Konfiguration bei Windows-Clients" auf Seite 65.
- Arbeitet der Protector im *PPPoE*-Modus, muss NAT aktiviert werden, um Zugriff auf das Internet zu erhalten - siehe „Filter → NAT" auf Seite 33. Ist NAT nicht aktiviert, können nur VPN-Verbindungen genutzt werden.

PPTP

Ähnlich dem *PPPoE*-Modus. In Österreich zum Beispiel wird statt des PPPoE-Protokolls das PPTP-Protokoll zur DSL-Anbindung verwendet.
(PPTP ist das Protokoll, das ursprünglich von Microsoft für VPN-Verbindungen benutzt worden ist.)

- Wird der Protector im *PPTP*-Modus betrieben, muss bei lokal angeschlossenen Client-Rechnern der Protector als Standardgateway festgelegt sein. D. h. die Adresse des Standardgateway ist auf die interne IP des Protector zu setzen. Siehe „☞ IP-Konfiguration bei Windows-Clients" auf Seite 65.
- Wird der Protector im *PPTP*-Modus betrieben, sollte NAT aktiviert werden, um aus dem lokalen Netz heraus Zugriff auf das Internet zu erhalten - siehe „Filter → NAT" auf Seite 33. Ist NAT nicht aktiviert, können nur VPN-Verbindungen genutzt werden.

Interne IPs

Interne IP ist die IP-Adresse, unter der der Protector von Geräten des lokal angeschlossenen lokalen Netzes erreichbar ist.

Im **Stealth**-Modus lautet diese immer:

IP-Adresse: **1.1.1.1**

Im **Router- / PPPoE- / PPTP**-Modus ist werksseitig voreingestellt:

IP-Adresse:	**192.168.1.1**
Lokale Netzmaske:	**255.255.255.0**

Sie können weitere Adressen festlegen, unter der der Protector von Geräten des lokal angeschlossenen Netzes angesprochen werden kann. Das ist zum Beispiel dann hilfreich, wenn das lokal angeschlossene Netz in Subnetze unterteilt wird. Dann können mehrere Geräte aus verschiedenen Subnetzen den Protector unter unterschiedlichen Adressen erreichen.

☞ Wollen Sie eine weitere interne IP festlegen, klicken Sie **Neu**.
Sie können beliebig viele interne IPs festlegen.

☞ Wollen Sie eine interne IP löschen, klicken Sie **Löschen**.
(Die erste IP-Adresse in der Liste können Sie nicht löschen.)

⌦ Weitere festgelegte interne IPs haben im *Stealth*-Modus keine Wirkung. Im Stealth-Modus lautet die IP-Adresse immer: 1.1.1.1

Zusätzliche interne Routen

Router- / PPPoE- / PPTP-Modus:

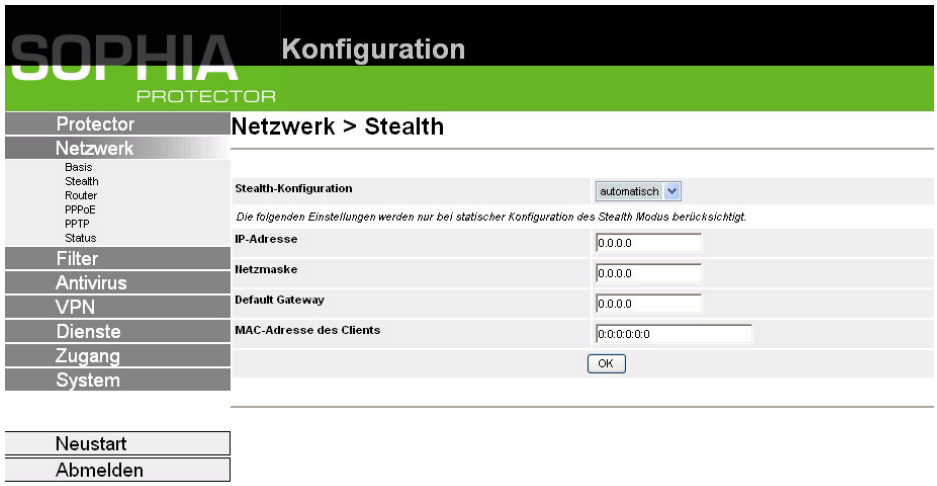
Sind am lokal angeschlossen Netz weitere Subnetze angeschlossen, können Sie zusätzliche Routen definieren.
Siehe auch „Netzwerk-Beispielskizze” auf Seite 78.

☞ Wollen Sie eine weitere Route zu einem Subnetz festlegen, klicken Sie **Neu**.
Geben Sie an:
- die IP-Adresse des Subnetzes (Netzwerkes), ferner
- die IP-Adresse des Gateways, über das das Subnetz angeschlossen ist.
Sie können beliebig viele interne Routen festlegen.

☞ Wollen Sie eine interne Route löschen, klicken Sie **Löschen**.

⌦ Sind zusätzliche interne Routen festgelegt, haben diese im *Stealth*-Modus keine Wirkung.

Netzwerk → Stealth



Voraussetzung: Der Protector ist auf den Netzwerk-Modus *Stealth* gestellt.

Stealth-Konfiguration

automatisch

(Standard) Der Protector analysiert den Netzwerkverkehr, der über ihn läuft, und konfiguriert dementsprechend seine Netzwerkanbindung eigenständig und arbeitet transparent.

Für Spezialfälle lassen sich diese Werte auch vorgeben, z. B. in folgendem Fall: Der angeschlossene Rechner nimmt nur eingehende Verbindungen entgegen, so dass keine automatische Konfiguration erfolgen kann.

statisch

Wenn der Protector keinen über ihn laufenden Netzwerkverkehr analysieren kann, z. B. weil zum lokal angeschlossenen Rechner nur Daten ein-, aber nicht ausgehen, dann muss die *Stealth-Konfiguration* auf **statisch** gesetzt werden.

In diesem Fall machen Sie zu folgenden Punkten die entsprechenden Angaben:

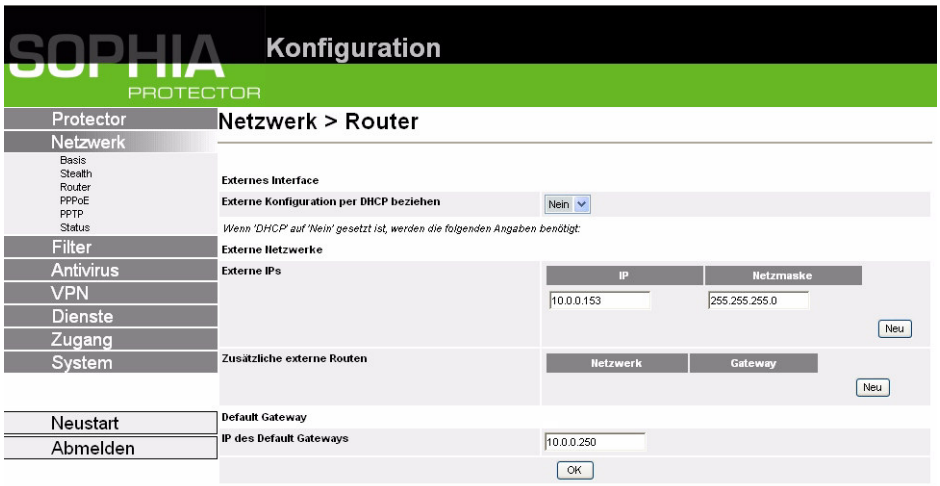
- **IP-Adresse** des angeschlossenen Clients
- **Netzmaske** des Clients
- **Default Gateway** des Clients
- **MAC-Adresse des Clients**. Das ist die physikalische Adresse der Netzwerkkarte des lokalen Rechners, an dem der Protector angeschlossen ist.

Die MAC-Adresse ermitteln Sie wie folgt:

Auf der DOS-Ebene (Menü **Start, Alle Programme, Zubehör, Eingabeaufforderung**) folgenden Befehl eingeben:

```
ipconfig  /all
```

Netzwerk → Router



Voraussetzung: Der Protector ist auf den Netzwerk-Modus *Router* gestellt..

Externes Interface

Externe Konfiguration per DHCP beziehen: Ja / Nein

☞ Falls der Protector die Konfigurationsdaten per DHCP (Dynamic Host Configuration Protocol) vom DHCP-Server bezieht, legen Sie **Ja** fest. Dann bleiben weiter Angaben auf dieser Seite wirkungslos.

☞ Falls der Protector die Daten nicht per DHCP (Dynamic Host Configuration Protocol) vom DHCP-Server bezieht, legen Sie **Nein** fest.
Der Protector muss dann im Netzwerk-Modus *Router* arbeiten - siehe „Router” auf Seite 23. Dann müssen Sie weiteren Angaben machen:

Externe Netzwerke

Externe IPs

Die Adressen, unter denen der Protector von Geräten des externen Netzes (angeschlossenen an der Ethernet-Buchse des Protector) aus ereichbar ist. Bildet die Schnittstelle zu anderen Teilen des LAN oder zum Internet. Findet hier der Übergang zum Internet statt, werden die IP-Adressen vom Internet Service Provider (ISP) vorgegeben.

☞ Wollen Sie eine weitere externe IP angeben, klicken Sie **Neu**.

☞ Wollen Sie eine der zusätzlichen externen IPs löschen, klicken Sie **Löschen**.

Zusätzliche externe Routen

Zusätzlich zur Default Route (s. u.) können Sie weitere externe Routen festlegen.

☞ Wollen Sie eine weitere externe Route angeben, klicken Sie **Neu**.

☞ Wollen Sie eine der zusätzlichen externen Routen löschen, klicken Sie **Löschen**.

Siehe auch „Netzwerk-Beispielskizze” auf Seite 78.

Default Gateway

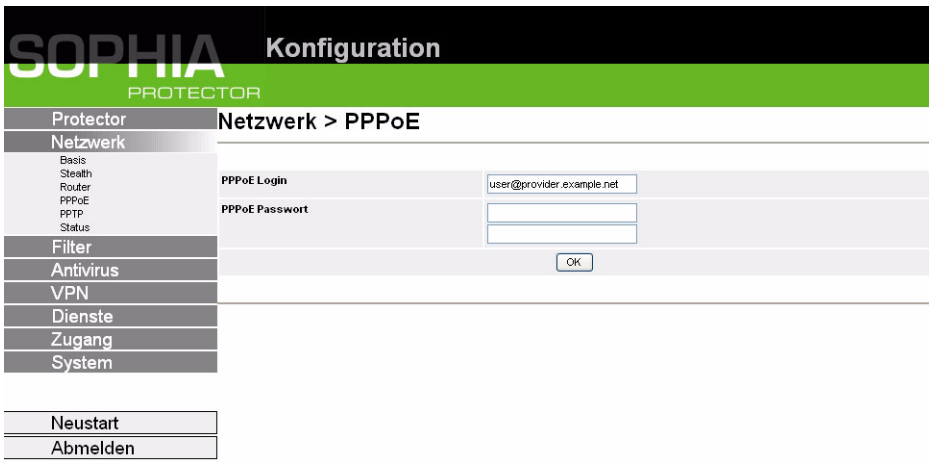
IP des Default Gateways

Wird vom Internet Service Provider (ISP) vorgegeben, wenn der Protector den Übergang zum Internet herstellt. Wird der Protector innerhalb des LANs eingesetzt, wird die Route vom Netzwerk-Administrator vorgegeben.

⌦ Das Default Gateway kann bei bestimmten Konfigurationen Teil des internen Netzes sein.

⌦ Wenn das lokale Netz dem externen Router nicht bekannt ist, z. B. im Falle einer Konfiguration per DHCP, dann sollten Sie unter Firewall → NAT Ihr lokales Netz angeben, also 0.0.0.0/0 (siehe „Filter → NAT” auf Seite 33)

Netzwerk → PPPoE



Voraussetzung: Der Protector ist auf den Netzwerk-Modus *PPPoE* gestellt. - siehe „PPPoE” auf Seite 24.

Benutzername (Login) und Passwort werden vom Internet Service Provider (ISP) abfragt, wenn Sie eine Verbindung ins Internet herstellen wollen.

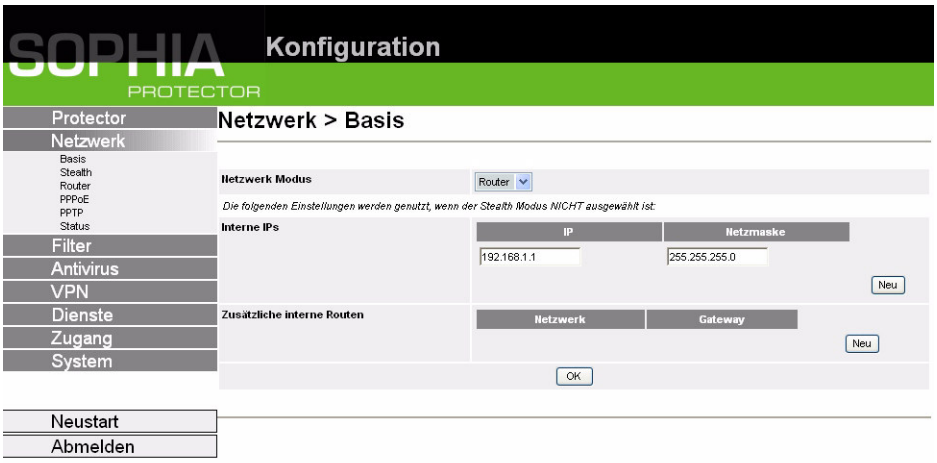
PPPoE Login

Benutzername (Login), den der Internet Service Provider (ISP) anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.

PPPoE Passwort

Passwort, das der Internet Service Provider anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.

Netzwerk → PPTP



Voraussetzung: Der Protector ist auf den Netzwerk-Modus *PPTP* gestellt. - siehe „PPTP" auf Seite 24.

Benutzername (Login) und Passwort werden vom Internet Service Provider (ISP) abfragt, wenn Sie eine Verbindung ins Internet herstellen wollen.

PPTP Login

Benutzername (Login), den der Internet Service Provider anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.

PPTP Passwort

Passwort, das der Internet Service Provider anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.

Setze lokale IP

Über DHCP

Werden die Adressdaten für den Zugang zum PPTP-Server vom Internet Service Provider per DHCP geliefert, wählen Sie **Über DHCP**.

Dann ist kein Eintrag unter **Lokale IP** zu machen.

Modem IP. Das ist die Adresse des PPTP-Servers des Internet Service Providers.

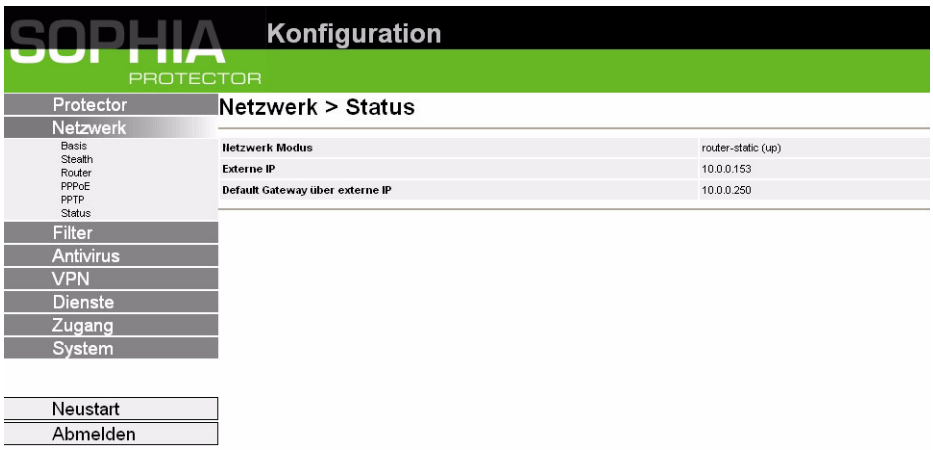
statisch (folgendes Feld)

Werden die Adressdaten für den Zugang zum PPTP-Server nicht per DHCP vom Internet Service Provider geliefert, dann muss die IP-Adresse gegenüber dem PPTP-Server angegeben werden - als lokale IP-Adresse.

Lokale IP. IP-Adresse, unter der der Protector vom PPTP-Server aus zu erreichen ist.

Modem IP. Das ist die Adresse des PPTP-Servers des Internet Service Providers.

Netzwerk → Status



Nur Anzeige

Netzwerk Modus

Zeigt die aktuelle Betriebsart des Protector: *Stealth, Router, PPPoE* oder *PPTP*. Siehe „Netzwerk → Basis" auf Seite 23.

Externe IP

Die IP-Adresse des Protector an seinem Anschluss für das externe Netz (WAN bzw. Internet).
Wird dem Protector eine IP-Adresse dynamisch zugeteilt, können Sie hier die gerade gültige IP-Adresse nachschlagen.
Im *Stealth*-Modus übernimmt der Protector die Adresse des lokal angeschlossenen Rechners für diese Schnittstelle.

Default Gateway über externe IP

Hier wird die externe IP-Adresse des Protector angezeigt. Im *Stealth*-Modus steht hier „(none)".

5.6 Menü Filter

Der Protector beinhaltet eine *Stateful Packet Inspection Firewall*. Die Verbindungsdaten einer aktiven Verbindung werden in einer Datenbank erfasst (connection tracking). Dadurch sind Regeln nur für eine Richtung zu definieren, Daten aus der anderen Richtung einer Verbindung, und nur diese, werden automatisch durchgelassen. Ein Nebeneffekt ist, dass bestehende Verbindungen bei einer Umkonfiguration nicht abgebrochen werden, selbst wenn eine entsprechende neue Verbindung nicht mehr aufgebaut werden dürfte.

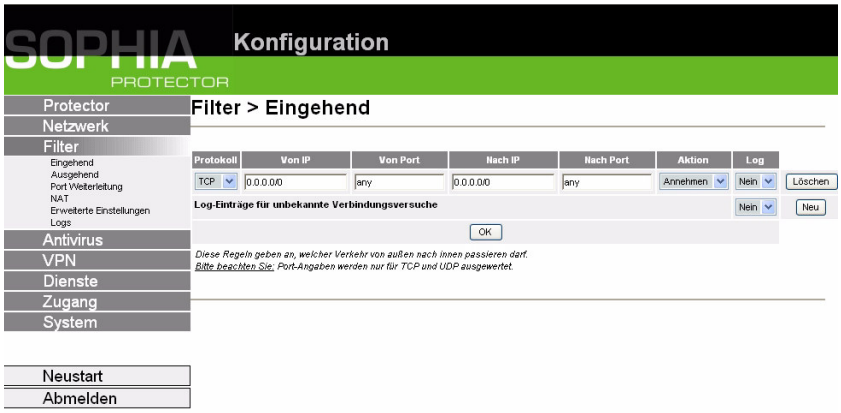
Werksseitige Voreinstellung der Firewall:

- Alle eingehenden Verbindungen werden abgewiesen (außer VPN).
- Die Datenpakete aller ausgehenden Verbindungen werden durchgelassen.

⌦ VPN-Verbindungen unterliegen nicht den unter diesem Menüpunkt festgelegten Firewall-Regeln. Firewall-Regeln für jede einzelne VPN-Verbindung können Sie unter Menü **VPN → Verbindungen** festlegen.

⌦ Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

Filter → Eingehend



Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenverbindungen, die von extern initiiert wurden.
Ist keine Regel gesetzt, werden alle eingehenden Verbindungen (außer VPN) abgewiesen (= Werkseinstellung).

⌦ Durch die Aktivierung der Antivirusfunktion (siehe "Menü Antivirus" auf Seite 36) werden implizit Firewallregeln für die Protokolle HTTP, SMTP und POP3 eingerichtet, die **nicht** in der Liste der Firewall-Regeln erscheinen.

Regel löschen

☞ Klicken Sie neben dem betreffenden Eintrag **Löschen**. Dann **OK**.

Neue Regel setzen

☞ Wollen Sie eine neue Regel setzen, klicken Sie **Neu**.
Legen Sie die gewünschte Regel fest (s. u.) und klicken Sie **OK**.
Zur Bestätigung erhalten Sie eine Systemmeldung.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll
Alle bedeutet: TCP, UDP, ICMP und andere IP-Protokolle.

IP-Adresse
0.0.0.0/0 bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)" auf Seite 77.

Port
(wird nur ausgewertet bei den Protokollen TCP und UDP)
any bezeichnet jeden beliebigen Port.
startport:endport (z. B. 110:120) bezeichnet einen Portbereich.
Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Aktion
Annehmen bedeutet, die Datenpakete dürfen passieren.
Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat Abweisen dieselbe Wirkung wie Verwerfen (s. u.).)
Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

⌦ Im Stealth-Modus ist **Abweisen** als Aktion nicht möglich.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

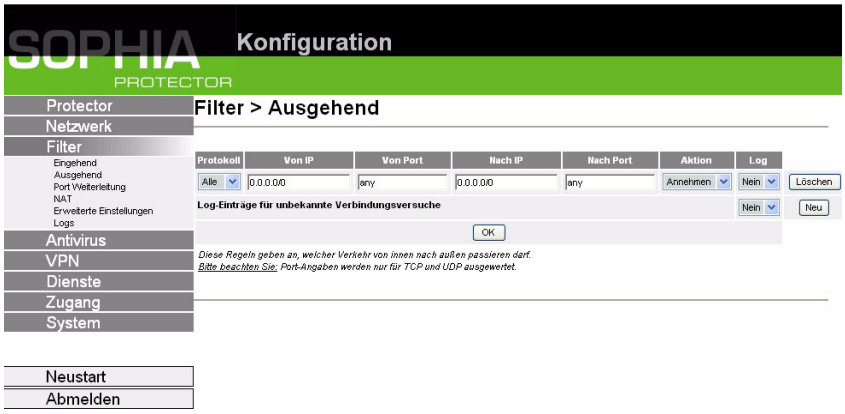
☞ das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen

☞ oder nicht - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

Log-Einträge für unbekannte Verbindungsversuche

Damit werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.

Filter → Ausgehend



Listet die eingerichteten Firewall-Regeln auf. Sie gelten für ausgehende Datenverbindungen, die von intern initiiert wurden, um mit einer entfernten Gegenstelle zu kommunizieren.

Per Werkseinstellung ist eine Regel gesetzt, die alle ausgehenden Verbindungen zulässt.

Ist keine Regel gesetzt, sind alle ausgehenden Verbindungen verboten (außer VPN).

Regel löschen

☞ Klicken Sie neben dem betreffenden Eintrag **Löschen**, dann **OK**.

Neue Regel setzen

☞ Wollen Sie eine neue Regel setzen, klicken Sie **Neu**.
Legen Sie die gewünschte Regel fest (s. u.) und klicken Sie **OK**
Zur Bestätigung erhalten Sie eine Systemmeldung.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll

Alle bedeutet: TCP, UDP, ICMP und andere IP-Protokolle.

IP-Adresse

0.0.0.0/0 bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)" auf Seite 77.

Port

(wird nur ausgewertet bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben, z. B. 110 für pop3 oder pop3 für 110.

Aktion

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat Abweisen dieselbe Wirkung wie *Verwerfen* (s. u.).)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

⌧ Im Stealth-Modus ist **Abweisen** als Aktion nicht möglich.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

☞ das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen

☞ oder nicht - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

Log-Einträge für unbekannte Verbindungsversuche

Damit werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.

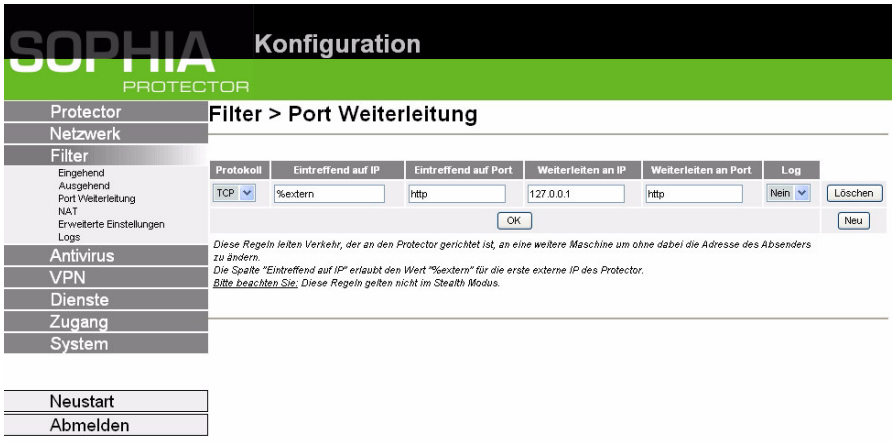
Filter → Port Weiterleitung

Listet die festgelegten Regeln zur Port-Weiterleitung auf.

Bei Port-Weiterleitung geschieht Folgendes: Der Header eingehender Datenpakete aus dem externen Netz, die an die externe IP-Adresse (oder eine der externen IP-Adressen) des Protector sowie an einen bestimmten Port des Protector gerichtet sind, werden so umgeschrieben, dass sie ins interne Netz an einen bestimmten Rechner und zu einem bestimmten Port dieses Rechners weitergeleitet werden. D. h. die IP-Adresse und Port-Nummer im Header eingehender Datenpakete werden geändert.

Dieses Verfahren wird auch Destination-NAT genannt.

⌧ Die hier eingestellten Regeln haben Vorrang gegenüber den Einstellungen unter **Firewall → Eingehend**.



Regel löschen

☞ Klicken Sie neben dem betreffenden Eintrag **Löschen**, dann **OK**.

Neue Regel setzen

☞ Wollen Sie eine neue Regel zu setzen, klicken Sie **Neu**.

Legen Sie die gewünschte Regel fest (s. u.) und klicken Sie **OK.**

Protokoll
Geben Sie hier das Protokoll an, auf den sich die Regel beziehen soll.

Eintreffend auf IP
Geben Sie hier die externe IP-Adresse (oder eine der externen IP-Adressen) des Protector an.
ODER
Falls ein dynamischer Wechsel der der externen IP-Adresse des Protector erfolgt, so dass diese nicht angebbar ist, verwenden Sie folgende Variable: **%extern.**

⌦ Die Angabe von **%extern** bezieht sich bei der Verwendung von mehreren statischen IP-Adressen für das externe Interface immer auf die erste IP-Adresse der Liste.

Eintreffend auf Port
Original-Ziel-Port, der in eingehenden Datenpaketen angegeben ist.

Weiterleiten an IP
Interne IP-Adresse, an die die Datenpakete weitergeleitet werden sollen und auf die die Original-Zieladressen umgeschrieben werden.

Weiterleiten an Port
Port, an den die Datenpakete weitergeleitet werden sollen und auf den die Original-Port-Angaben umgeschrieben werden.

Bei den Angaben haben Sie folgende Möglichkeiten:

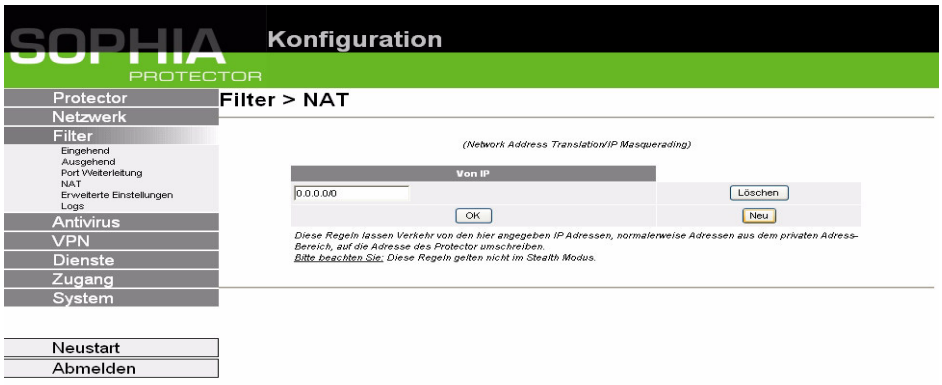
Port
Sie können nur einzelne Ports angeben, entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen: (z. B. 110 für pop3 oder pop3 für 110).

Log
Für jede einzelne Port-Weiterleitungs-Regel können Sie festlegen, ob bei Greifen der Regel

☞ das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen

☞ oder nicht - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

Filter → NAT



Listet die festgelegten Regeln für NAT (**N**etwork **A**ddress **T**ranslation) auf.
Das Gerät kann bei ausgehenden Datenpaketen die angegebenen Absender-IP-Adressen aus seinem internen Netzwerk auf seine eigene externe Adresse umschreiben, eine Technik, die als NAT (Network Address Translation) bezeichnet wird.

Diese Methode wird benutzt, wenn die internen Adressen extern nicht geroutet werden können oder sollen, z. B. weil ein privater Adressbereich wie 192.168.x.x oder weil die interne Netzstruktur verborgen werden soll.
Dieses Verfahren wird auch *IP-Masquerading* genannt.

- Arbeitet der Protector im *PPPoE/PPTP*-Modus, muss NAT aktiviert werden, um Zugriff auf das Internet zu erhalten. Ist NAT nicht aktiviert, können nur VPN-Verbindungen genutzt werden.
- Bei der Verwendung von mehreren statischen IP-Adressen für das externe Interface wird immer die erste IP-Adresse der Liste für IP-Masquerading verwendet.

Werkseinstellung: Es findet kein NAT statt.

Regel löschen

☞ Klicken Sie neben dem betreffenden Eintrag **Löschen**, dann **OK**.

Neue Regel setzen

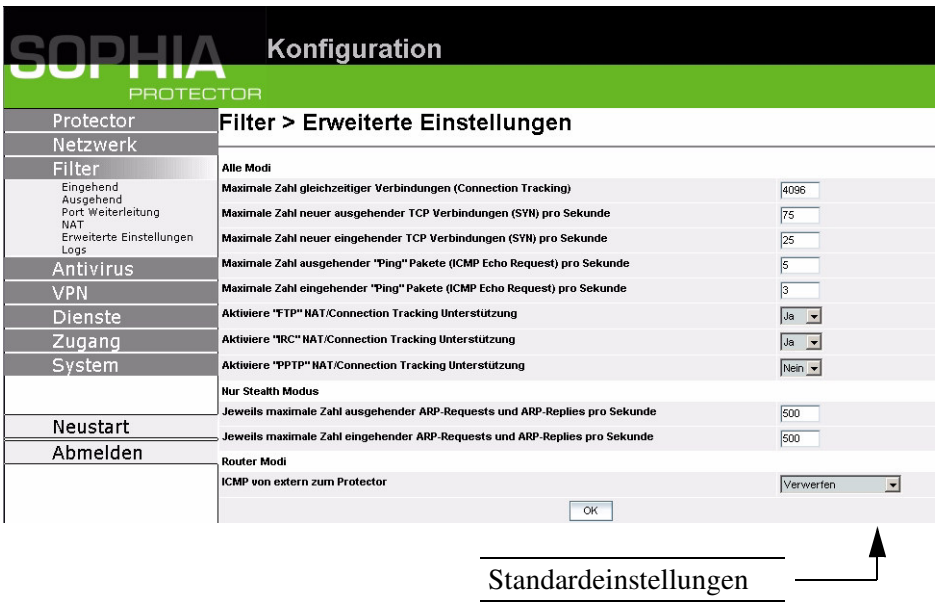
☞ Wollen Sie eine neue Regel setzen, klicken Sie **Neu**.
Legen Sie die gewünschte Regel fest (s. u.) und klicken Sie **OK**.

Bei den Angaben haben Sie folgende Möglichkeiten:

Von IP

0.0.0.0/0 bedeutet alle Adressen, d. h. alle internen IP-Adressen werden dem NAT-Verfahren unterzogen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)" auf Seite 77.

Filter → Erweiterte Einstellungen



Die Einstellungen betreffen das grundlegende Verhalten der Firewall.

Alle Modi

Maximale Zahl ...

Diese 5 Einträge legen Obergrenzen fest. Diese sind so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte erhöhen.

Aktiviere „FTP“ NAT/Connection Tracking Unterstützung

Wird beim FTP-Protokoll eine ausgehende Verbindung hergestellt, um Daten abzurufen, gibt es zwei Varianten der Datenübertragung: Beim „aktiven FTP“ stellt der angerufene Server im Gegenzug eine zusätzliche Verbindung zum Anrufer her, um auf dieser Verbindung die Daten zu übertragen. Beim „passiven FTP“ baut der Client diese zusätzliche Verbindung zum Server zur Datenübertragung auf. Damit die zusätzlichen Verbindungen von der Firewall durchgelassen werden, muss **Aktiviere „FTP“ NAT/Connection Tracking Unterstützung** auf **Ja** stehen (Standard).

Aktiviere „IRC“ NAT/Connection Tracking Unterstützung

Ähnlich wie bei FTP: Beim Chatten im Internet per IRC müssen nach aktivem Verbindungsaufbau auch eingehende Verbindungen zugelassen werden, soll das Chatten reibungslos funktionieren. Damit diese von der Firewall durchgelassen werden, muss **Aktiviere „IRC“ NAT/Connection Tracking Unterstützung** auf **Ja** stehen (Standard).

Aktiviere „PPTP“ NAT/Connection Tracking Unterstützung

Muss nur dann auf **Ja** gesetzt werden, wenn folgende Bedingung vorliegt: Von einem lokalen Rechner soll ohne Zuhilfenahme des Protector eine VPN-Verbindung mittels PPTP zu einem externen Rechner aufgebaut werden.

Werksseitig ist dieser Schalter auf **Nein** gesetzt.

Nur Stealth Modus

Jeweils maximale Zahl ausgehender ARP-Requests ...

Jeweils maximale Zahl eingehender ARP-Requests ...

Diese beiden Einträge legen Maximalwerte für die zugelassenen ein- und ausgehenden ARP-Requests pro Sekunde fest. Diese sind so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte erhöhen.

Router Modi

ICMP von extern zum Protector

Mit dieser Option können Sie das Verhalten beim Empfang von ICMP-Nachrichten beeinflussen, die aus dem externen Netz an den Protector gesendet werden. Sie haben folgende Möglichkeiten:

Verwerfen: Alle ICMP-Nachrichten zum Protector werden verworfen.

Annehmen von Ping: Nur Ping-Nachrichten (ICMP Typ 8) zum Protector werden akzeptiert.

Alle ICMPs annehmen: Alle Typen von ICMP Nachrichten zum Protector werden akzeptiert.

Filter → Logs

Nur Anzeige

Ist bei Festlegung von Firewall-Regeln das Protokollieren von Ereignissen festgelegt (Log = Ja), dann können Sie hier das Log aller protokollierten Ereignisse einsehen.

Das Format entspricht dem unter Linux gebräuchlichen Format.

Es gibt spezielle Auswertungsprogramme, die Ihnen die Informationen aus den protokollierten Daten in einem besser lesbaren Format präsentieren.

5.7 Menü Antivirus

Der Antivirus-Funktion des SOPHIA Protector schützt vor Viren, die über die Protokolle HTTP, POP3 und SMTP versendet werden.

Kaspersky Engine

Die übertragenenen Datenblöcke einer E-Mail oder einer HTTP-Verbindung werden aus dem Datentransfer ausgefiltert, falls notwendig dekomprimiert, und durch den Kaspersky-Virenfilter überprüft.
Dazu wird für jedes unterstützte Protokoll eine Port-Redirection-Regel in die Firewall eingefügt, die eine interne Umleitung der Verbindung zu einem transparenten Proxy bewirkt.
Im Falle eines erkannten Virus wird je nach Protokoll entweder eine Fehlermeldung als E-Mail an den Nutzer gesendet, eine Protokollfehlermeldung generiert bzw. ein Eintrag im Antivirus-Log vorgenommen. Falls der Virenfilter keinen Virus findet, wird der Datenblock vom Proxy unverändert weitergesendet.
Details erfahren Sie in den folgenden Abschnitten zu den jeweiligen Protokollen.

⌦ Der Antivirus-Schutz ist gegenwärtig nur im Routermodus des Protector funktionsfähig!

Unterstützte Kompressionformate

Der Virenfilter kann folgende Formate dekomprimieren:

- ZIP
- RAR
- Mail
- Embedded (RFC822 MIME Anhänge an E-Mails, MS OLE, inklusive gzipped embedded Skripte).
- GZIP
- Compress

Die Unterstützung weiterer Formate (Trap, UPX) ist in Vorbereitung.

Voraussetzungen zur Nutzung

Folgende Voraussetzungen müssen für die Nutzung des Virenfilters erfüllt sein:

- Installierte Antiviren-Lizenz. Nur mit installierter Lizenz ist das Menü „Antivirus“ aktiviert. Die Anleitung, wie Sie eine Lizenz anfordern und installieren, finden Sie im Abschnitt **Antivirus->Lizenzanforderung**.
- Zugriff auf einen Update-Server mit den aktuellen Versionen der Virensignaturen (siehe Abschnitt **Antivirus->Datenbank-Update**).
- Konfiguration des Protector im Routermodus (siehe “Menü Netzwerk” auf Seite 23).
- Konfiguration und Aktivierung des Antiviren-Schutzes (siehe folgende Abschnitte für die jeweiligen Protokolle)

Dateigrößenbegrenzung

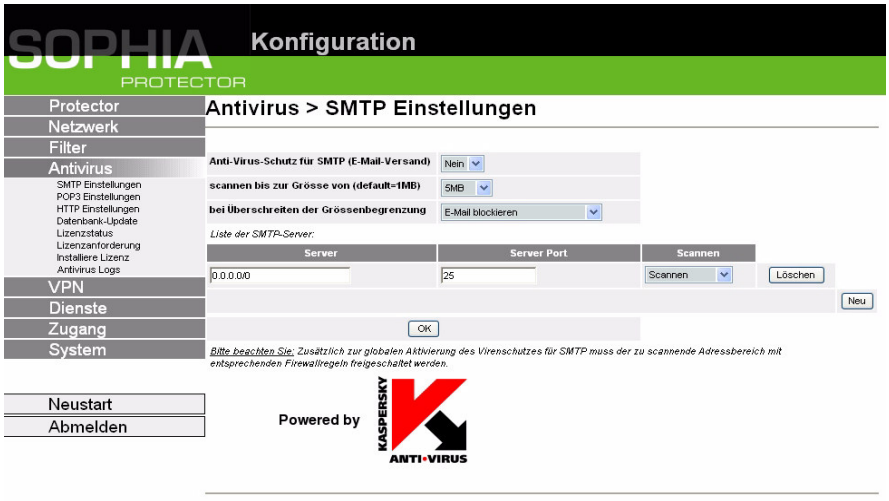
Durch die begrenzte Speicherkapazität des SOPHIA Protector ergeben sich einige zu beachtende Unterschiede zu üblichen Virenfiltern.
Jede zu überprüfende Datei muß komplett auf die Protector-RAM-Disk kopiert werden, damit sie durch den Virenfilter dekomprimiert und auf Viren untersucht werden kann. Da der SOPHIA Protector mehrere Verbindungen gleichzeitig überwacht, um z.B. parallel E-Mail-Clients und Web-Browser nutzen zu können, kann es zu Speicher-Engpäßen kommen. Um diesen Engpässen vorzubeugen, muss im Menü die Maximalgröße der zu überprüfenden Dateien festgelegt werden. Mit den voreingestellten Werten für die Maximalgröße ist in den meisten Szenarien ein problemloser Betrieb des Antivirenfilters möglich, deswegen sollten Sie diese Werte möglichst nicht ändern.
Sie können im Menü auswählen, ob bei einer Überschreitung der Maximalgröße die Nachricht blockiert und eine Fehlermeldung an Sie gesendet werden soll, oder ob die Datei ohne Virenüberprüfung weitergeleitet werden soll.

Antivirus → SMTP-Einstellungen

Das SMTP-Protokoll wird von Ihrem E-Mail-Client oder Mail-Transfer-Agent (MTA) zur Versendung von E-Mails genutzt.

Konfiguration des E-Mail-Clients / Meldungen des Virenfilters

Der Virenfilter kann nur unverschlüsselte Daten auf Viren untersuchen. Deshalb sollten Sie Verschlüsselungsoptionen wie TLS nicht aktivieren. Im Falle der Detektion eines Virus oder beim Auftreten von Fehlern wird der E-Mail-Client des Absenders durch einen Fehlercode benachrichtigt und ein Logeintrag im Antivirus-Log vorgenommen. Der ursprüngliche Empfänger erhält weder die infizierte Mail noch eine Benachrichtigung.



Anti-Virus-Schutz für SMTP (E-Mail-Versand)

Mit dieser Option aktivieren Sie den Virenfilter (Auf „Ja setzen) oder deaktivieren den Filter (Auf „Nein“ setzen). Bei einer Aktivierung wird eine Port-Redirection für SMTP-Verbindungen auf den SMTP-Proxy angelegt.

⌦ Wird der Virenfilter während einer aktiven Verbindung aktiviert oder deaktiviert, so gilt die alte Einstellung, bis das laufende Protokoll dieser Verbindung beendet ist.

scannen bis zur Grösse von (default=1MB)

Hier geben Sie die Maximalgöße in MBytes der zu überprüfenden Dateien an. Wird diese Grenze überschritten, wird abhängig von der Einstellung „bei Überschreitung der Grössenbegrenzung“ eine Fehlermeldung an den E-Mail-Client zurückgegeben und die E-Mail nicht gesendet oder automatisch in den Durchlaßmodus geschaltet.

Wenn die Speicherkapazität des Protector nicht ausreicht, um die Datei vollständig zu speichern oder zu dekomprimieren, wird eine entsprechende Fehlermeldung an die Client-Software (Browser, Download-Manager) des Benutzers ausgegeben und ein Eintrag im Antivirus-Log vorgenommen. In diesem Fall haben Sie folgende Optionen:

- Sie können versuchen, den Download zu einem späteren Zeitpunkt zu wiederholen
- Sie können den Virenfilter für den betreffenden Server kurzzeitig deaktivieren
- Sie können die Option für den automatischen Durchlaßmodus aktivieren.

Bitte beachten Sie, dass die Größe des Anhangs je nach Kodierung u.U. ein Vielfaches der ursprünglichen Datei sein kann.

bei Überschreiten der Grössenbegrenzung

E-Mail ungescannt durchlassen

Diese Option bewirkt ein automatisches Umschalten des Virenfilters in den Durchlaßmodus, wenn die eingestellte Dateigröße überschritten wird.

⌦ In diesem Fall wird nicht auf Viren überprüft!

E-Mail blockieren

Diese Option bewirkt die Ausgabe eines Fehlercodes an den E-Mail-Client und das Blockieren der E-Mail.

Liste der SMTP Server

Sie können die Server angeben, deren Datenverkehr gefiltert werden soll und für jede IP explizit angeben, ob der Antivirus-Schutz aktiviert werden soll oder nicht. Dadurch ist auch die Angabe von "trusted" Servern möglich.

Beispiele:
Globale Aktivierung des Antivirus-Schutzes für SMTP:

Server	Server Port	Scannen
0.0.0.0/0	25	Scannen

Scan eines Subnetzes, Ausklammerung eines "trusted" SMTP-Servers:

Server	Server Port	Scannen
192.168.2.5	25	Nicht Scannen
192.168.2.0/24	25	Scannen

Scan eines einzelnen "untrusted" SMTP-Servers in einem Subnetz:

Server	Server Port	Scannen
192.168.2.5	25	Scannen
192.168.2.0/24	25	Nicht Scannen

Regel löschen

☞ Klicken Sie neben dem betreffenden Eintrag **Löschen**, dann **OK**.

Neue Regel setzen

☞ Wollen Sie eine neue Regel setzen, klicken Sie **Neu**.
Legen Sie die gewünschte Regel fest (s. u.) und klicken Sie **OK**.

⌦ Der Regelsatz wird wie bei der Angabe der Firewallregeln von oben nach unten abgearbeitet, die Reihenfolge der Regeln ist also auschlaggebend für das Ergebnis.

⌦ Der Virenfilter kann parallel insgesamt bis zu 50 gleichzeitige Verbindungen zu Mail-Servern und HTTP-Servern verarbeiten. Wird diese Zahl überschritten, dann wird jeder weitere Verbindungsversuch abgelehnt.

Bei den Angaben haben Sie folgende Möglichkeiten:

Server

0.0.0.0/0 bedeutet alle Adressen, d. h. der Datenverkehr aller SMTP-Server wird gefiltert. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)” auf Seite 77.

⌦ Da ein Verbindungswunsch zunächst durch den Proxy entgegengenommen wird, reagiert die Benutzersoftware bei einer Anfrage an einen nicht-existen-

ten Server (z.B. falsche IP-Adresse) so, als ob die Serververbindung aufgebaut wird, aber keine Daten gesendet werden. Durch die genaue Angabe der Serveradressen in der Liste wird dieses Verhalten verhindert, da der Proxy nur Anfragen an die in der Liste angegebenen Adressen entgegennimmt.

Server Port

Hier geben Sie bitte die Nummer des Ports für das SMTP-Protokoll an. Der SMTP-Standardport **25** ist bereits voreingestellt.

⌦ Das Einschalten des SMTP Virenfilters öffnet die Firewall für die entsprechenden Ports unabhängig von zusätzlichen anderslautenden Firewall-Regeln.

Scannen

Scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server aktiviert.

Nicht scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server deaktiviert.

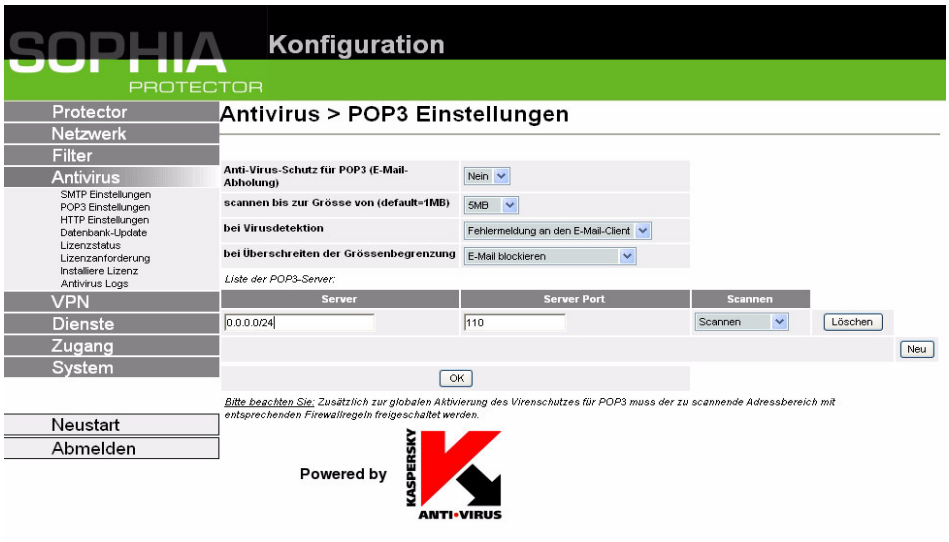
⌦ Eine Deaktivierung des Virenfilters erfolgt erst nachdem die laufende Verbindung beendet wurde. Deshalb sollten Sie nach einer Veränderung der Einstellungen des Virenfilters einen bereits laufenden SMTP-E-Mail-Transfer beenden.

Antivirus → POP3-Einstellungen

Das POP3-Protokoll wird von Ihrem E-Mail-Client zum Empfang von E-Mails genutzt

Konfiguration des E-Mail-Clients

Der Virenfilter kann nur unverschlüsselte Daten auf Viren untersuchen. Deshalb sollten Sie Verschlüsselungsoptionen wie STLS oder SSL nicht aktivieren. Die verschlüsselte Authentifizierung mittels AUTH ist dagegen nutzbar, da die eigentliche Übertragung der E-Mail unverschlüsselt erfolgt.



Anti-Virus-Schutz für POP3 (E-Mail-Abholung)

Mit dieser Option aktivieren Sie den Virenfilter (Auf „Ja setzen) oder deaktivieren den Filter (Auf „Nein“ setzen). Bei einer Aktivierung wird eine Port-Redirection für POP3-Verbindungen auf den POP3-Proxy angelegt.

⌦ Wird der Virenfilter während einer aktiven Verbindung aktiviert oder deaktiviert, so gilt die alte Einstellung, bis das laufende Protokoll dieser Verbindung

beendet ist.

⌦ Tip: Bei einer POP3-Verbindung werden durch die meisten E-Mail-Clients alle E-Mails über eine Verbindung abgerufen, so daß die neue Einstellung erst gilt, wenn die letzte Mail der aktuellen Verbindung von diesem Server abgerufen wurde. Um also während eines laufenden E-Mail-Transfers Einstellungen zu verändern, sollte der Transfer zunächst abgebrochen werden.

scannen bis zur Grösse von (default=1MB)

Hier geben Sie die Maximalgöße in MBytes der zu überprüfenden Dateien an. Wird diese Grenze überschritten, wird abhängig von der Einstellung „bei Überschreiten der Größenbegrenzung“ eine Fehlermeldung an den E-Mail-Client gesendet und die E-Mail nicht empfangen oder automatisch in den Durchlaßmodus geschaltet.

Wenn die Speicherkapazität des Protector nicht ausreicht, um die Datei vollständig zu speichern oder zu dekomprimieren, wird eine entsprechende Fehlermeldung an die Client-Software (Browser, Download-Manager) des Benutzers ausgegeben und ein Eintrag im Antivirus-Log vorgenommen. In diesem Fall haben Sie folgende Optionen:

- Sie können versuchen, den Download zu einem späteren Zeitpunkt zu wiederholen
- Sie können den Virenfilter für den betreffenden Server kurzzeitig deaktivieren
- Sie können die Option für den automatischen Durchlaßmodus aktivieren.

Bitte beachten Sie, dass die Größe des Anhangs je nach Kodierung u.U. ein Vielfaches der ursprünglichen Datei sein kann.

bei Virusdetektion

Benachrichtigung per E-Mail

Erkennt der Virenfilter einen Virus, dann wird der Empfänger durch eine E-Mail benachrichtigt.

Fehlermeldung an den E-Mail Client

Erkennt der Virenfilter einen Virus, dann wird der Empfänger durch eine Fehlermeldung an den E-Mail-Client benachrichtigt.

⌦ Ist für die E-Mail-Client-Software die Option "Gelesene E-Mails auf dem Server löschen" aktiviert, so wird bei der Einstellung "Benachrichtigung per E-Mail" die infizierte Mail auf dem Server gelöscht, da der E-Mail-Client davon ausgeht, daß die E-Mail erfolgreich übertragen wurde. Ist dies nicht gewünscht (wenn z.B. die infizierte E-Mail auf anderem Weg heruntergeladen werden soll), sollte ausschließlich die Option "Fehlermeldung an den E-Mail Client" genutzt werden.

bei Überschreiten der Grössenbegrenzung

E-Mail ungescannt durchlassen

Diese Option bewirkt ein automatisches Umschalten des Virenfilters in den Durchlaßmodus, wenn die eingestellte Dateigröße überschritten wird.

⌦ In diesem Fall findet keine Überprüfung auf Viren statt!

E-Mail blockieren

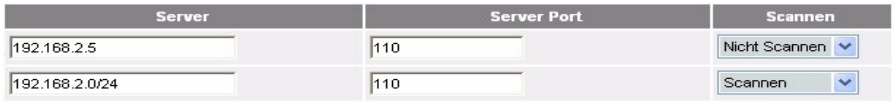
Diese Option bewirkt die Ausgabe eines Fehlercodes an den E-Mail-Client und das Blockieren der E-Mail.

Liste der POP3 Server

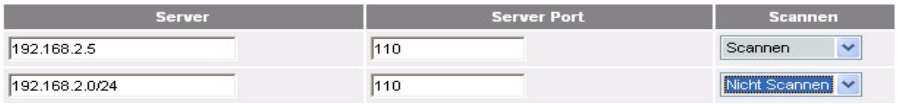
Sie können die Server auswählen, deren Datenverkehr gefiltert werden soll und für jede IP explizit angeben, ob der Antivirus-Schutz aktiviert werden soll oder nicht. Dadurch ist auch die Angabe von "trusted" Servern möglich.

Beispiele:
Globale Aktivierung des Antivirus-Schutzes für POP3:

Scan eines Subnetzes, Ausklammerung eines "trusted" POP3-Servers:



Scan eines einzelnen "untrusted" POP3 Servers in einem Subnetz:



Regel löschen

☞ Klicken Sie neben dem betreffenden Eintrag **Löschen**, dann **OK**.

Neue Regel setzen

☞ Wollen Sie eine neue Regel setzen, klicken Sie **Neu**.
Legen Sie die gewünschte Regel fest (s. u.) und klicken Sie **OK**.

⌦ Der Regelsatz wird wie bei der Angabe der Firewallregeln von oben nach unten abgearbeitet, die Reihenfolge der Regeln ist also auschlaggebend für das Ergebnis.

⌦ Der Virenfilter kann parallel insgesamt bis zu 50 gleichzeitige Verbindungen zu Mail-Servern und HTTP-Servern verarbeiten. Wird diese Zahl überschritten, dann wird jeder weitere Verbindungsversuch abgelehnt.

Bei den Angaben haben Sie folgende Möglichkeiten:

Server

0.0.0.0/0 bedeutet alle Adressen, d. h. der Datenverkehr aller POP3-Server wird gefiltert. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)” auf Seite 77.

⌦ Da ein Verbindungswunsch zunächst durch den Proxy entgegengenommen wird, reagiert die Benutzersoftware bei einer Anfrage an einen nicht-existenten Server (z.B. falsche IP-Adresse) so, als ob die Serververbindung aufgebaut wird, aber keine Daten gesendet werden. Durch die genaue Angabe der Serveradressen in der Liste wird dieses Verhalten verhindert, da der Proxy nur Anfragen an die in der Liste angegebenen Adressen entgegennimmt.

Server Port

Hier geben Sie bitte die Nummer des Ports für das POP3-Protokoll an. Der POP3-Standardport **110** ist bereits voreingestellt.

⌦ Das Einschalten des POP3 Virenfilters öffnet die Firewall für die entsprechenden Ports unabhängig von zusätzlichen anderslautenden Firewall-Re-

geln.

Scannen

Scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server aktiviert.

Nicht scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server deaktiviert.

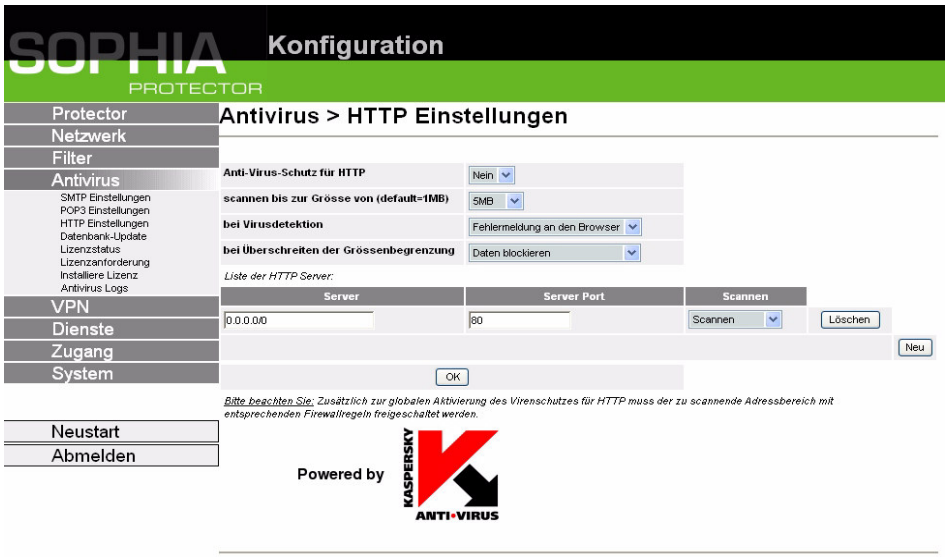
⌦ Eine Deaktivierung des Virenfilter erfolgt erst nachdem die laufende Verbindung beendet wurde. Deshalb sollten Sie nach einer Veränderung der Einstellungen des Antivirenfilters einen bereits laufenden POP3-E-Mail-Transfer beenden.

Antivirus → HTTP-Einstellungen

Das HTTP-Protokoll wird von Web-Browsern zur Übertragung von Webseiten genutzt, hat aber noch viele andere Anwendungen. So wird es z.B. auch zum Download von Dateien wie z.B. Software-Updates oder zur Initialisierung von Multimedia-Streams genutzt.

Die Weiterleitung einer übertragenen Datei erfolgt erst, nachdem sie komplett geladen und überprüft wurde. Deshalb kann es bei größeren Dateien oder einer langsamen Download-Geschwindigkeit zu Verzögerungen in der Reaktionszeit der Benutzer-Software kommen.

⌦ Um den Anti-Virus-Schutz für HTTP zu testen, bietet sich zunächst der ungefährliche Eicar-Testvirus an, der eigens für Testzwecke unter der Adresse http://www.eicar.org/anti_virus_test_file.htm heruntergeladen werden kann.



Anti-Virus-Schutz für HTTP

Mit dieser Option aktivieren Sie den Virenfilter (Auf „Ja setzen) oder deaktivieren den Filter (Auf „Nein“ setzen). Bei einer Aktivierung wird eine Port-Redirection für SMTP-Verbindungen auf den HTTP-Proxy angelegt.

⌦ Wird der Virenfilter während einer aktiven Verbindung aktiviert oder deaktiviert, so gilt die alte Einstellung, bis das laufende Protokoll dieser Verbindung beendet ist.

scannen bis zur Grösse von (default=1MB)

Hier geben Sie die Maximalgöße in MBytes der zu überprüfenden Dateien an. Wird diese Grenze überschritten, wird eine Fehlermeldung an den Browser gesendet oder automatisch in den Durchlaßmodus geschaltet.

Wenn die Speicherkapazität des Protector nicht ausreicht, um die Datei vollständig zu speichern oder zu dekomprimieren, wird eine entsprechende Fehlermeldung an die Client-Software (Browser, Download-Manager) des Benutzers ausgegeben und ein Eintrag im Antivirus-Log vorgenommen. In diesem Fall haben Sie folgende Optionen:

- Sie können versuchen, den Download zu einem späteren Zeitpunkt zu wiederholen
- Sie können den Virenfilter für den betreffenden Server kurzzeitig deaktivieren
- Sie können die Option für den automatischen Durchlaßmodus aktivieren.

bei Virusdetektion

Fehlermeldung an den Browser

Erkennt der Virenfilter einen Virus innerhalb eines Datentransfers vom HTTP-Server zum HTTP-Client, dann wird eine Fehlermeldung an den HTTP-Client gesendet. Die Darstellung dieser Fehlermeldung hängt vom jeweiligen HTTP-Client ab. Ein Webbrowser wird die Fehlermeldung in Form einer HTML-Seite darstellen. Ist eine innerhalb einer HTML-Seite nachgeladene Datei - z.B. eine Bilddatei - infiziert, so wird diese Datei im Browser nicht angezeigt. Wird ein Dateidownload per HTTP mittels Download-Manager vorgenommen, so wird die Fehlermeldung im Download-Manager angezeigt.

bei Überschreiten der Grössenbegrenzung

Daten ungescannt durchlassen

Diese Option bewirkt ein automatisches Umschalten des Virenfilters in den Durchlaßmodus, wenn die eingestellte Dateigröße überschritten wird.

⌦ In diesem Fall wird nicht auf Viren überprüft!

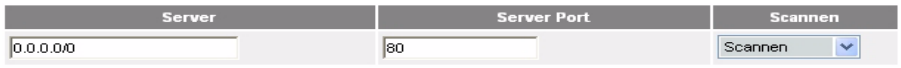
Daten blockieren

Diese Option bewirkt den Abbruch des Downloads und die Ausgabe eines Fehlercodes an die Client-Software.

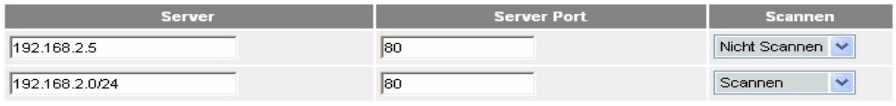
Liste der HTTP Server

Sie können die Server auswählen, deren Datenverkehr gefiltert werden soll und für jede IP explizit angeben, ob der Antivirus-Schutz aktiviert werden soll oder nicht. Dadurch ist auch die Angabe von "trusted" Servern möglich.

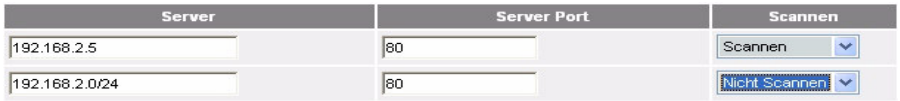
Beispiele:
Globale Aktivierung des Antivirus-Schutzes für HTTP:



Scan eines Subnetzes, Ausklammerung eines "trusted" HTTP-Servers:



Scan eines einzelnen "untrusted" HTTP-Servers in einem Subnetz:



Regel löschen

☞ Klicken Sie neben dem betreffenden Eintrag **Löschen**, dann **OK**.

Neue Regel setzen

☞ Wollen Sie eine neue Regel setzen, klicken Sie **Neu**.
Legen Sie die gewünschte Regel fest (s. u.) und klicken Sie **OK**.

⌦ Der Regelsatz wird wie bei der Angabe der Firewallregeln von oben nach unten abgearbeitet, die Reihenfolge der Regeln ist also auschlaggebend für das Ergebnis.

⌦ Der Virenfilter kann parallel insgesamt bis zu 50 gleichzeitige Verbindungen zu Mail-Servern und HTTP-Servern verarbeiten. Wird diese Zahl überschritten, dann wird jeder weitere Verbindungsversuch abgelehnt.

Bei den Angaben haben Sie folgende Möglichkeiten:

Server

0.0.0.0/0 bedeutet alle Adressen, d. h. der Datenverkehr aller HTTP-Server wird gefiltert. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)" auf Seite 77.

⌦ Da ein Verbindungswunsch zunächst durch den Proxy entgegengenommen wird, reagiert die Benutzersoftware bei einer Anfrage an einen nicht-existenten Server (z.B. falsche IP-Adresse) so, als ob die Serververbindung aufgebaut wird, aber keine Daten gesendet werden. Durch die genaue Angabe der Serveradressen in der Liste wird dieses Verhalten verhindert, da der Proxy nur Anfragen an die in der Liste angegebenen Adressen entgegennimmt.

Server Port

Hier geben Sie bitte die Nummer des Ports für das HTTP-Protokoll an. Der HTTP-Standardport **80** ist bereits voreingestellt.

⌦ Das Einschalten des HTTP Virenfilters öffnet die Firewall für die entsprechenden Ports unabhängig von zusätzlichen anderslautenden Firewall-Regeln.

Scannen

Scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server aktiviert.

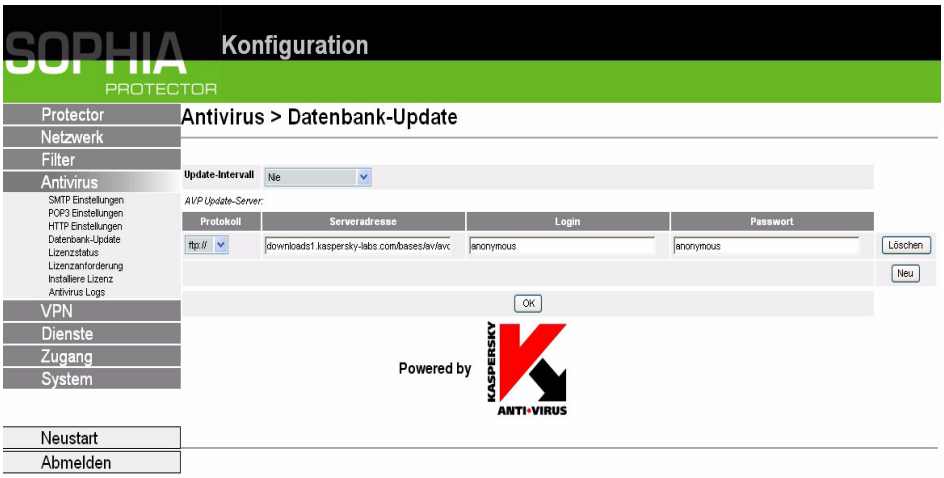
Nicht scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server deaktiviert.

⌦ Eine Deaktivierung des Virenfilters erfolgt erst nachdem die laufende Verbindung beendet wurde. Deshalb sollten Sie nach einer Veränderung der Einstellungen des Virenfilters alle Browser-Fenster schließen.

Antivirus → Datenbank-Update

Die Virensignaturdateien können durch einen einstellbaren Update-Server in einem nutzerdefinierten Intervall aktualisiert werden. Das Update geschieht parallel zur Nutzung des Antivirenfilters. Im Auslieferungszustand befinden sich keine Virensignaturen auf dem Protector. Deshalb sollte nach dem Aktivieren des Antiviren-Schutzes mit der entsprechenden Lizenz auch das Update-Intervall eingestellt werden. Der Verlauf des Updates kann im Antivirus-Log verfolgt werden.



Update-Intervall

Mit dieser Option wählen Sie das Aktualisierungsintervall der Signaturdateien. Die Größe der Datei beträgt z.Zt. etwa 3 MByte. Es werden nur die auf dem Update-Server aktualisierten Dateien nachgeladen.

AVP Update Server

Sie können die Server auswählen, von denen der Update der Virensignaturdatei geladen werden soll. Ein Standardserver ist bereits voreingetragen. Sie können bei Bedarf eigene Server angeben.

⌦ Die Liste der Server wird priorisiert von oben nach unten abgearbeitet, bis ein verfügbarer Server gefunden wurde.

Server löschen

☞ Klicken Sie neben dem betreffenden Eintrag **Löschen**, dann **OK**.

Server hinzufügen

☞ Wollen Sie einen neuen Server hinzufügen, klicken Sie **Neu**.
Geben Sie die Daten des Servers an (s. u.) und klicken Sie **OK**.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll

Der Update der Virensignaturdateien kann entweder per FTP oder HTTP erfolgen.

Server Adresse

FQDN oder IP-Adresse des Servers inclusive des vollen Pfadnames des Verzeichnisses, in der sich die Signaturdatei befindet.

Login

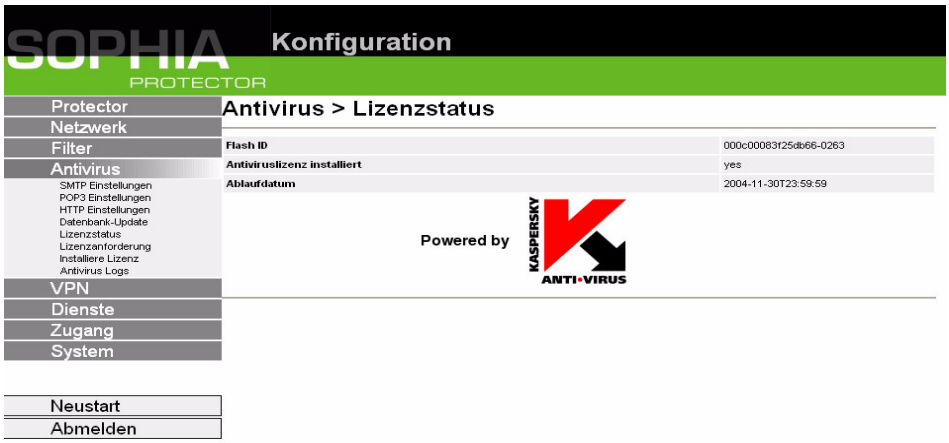
Login für den Server. Beim Update mittels HTTP-Protokoll ist eine Angabe des Logins u.U. nicht erforderlich.

Passwort

Passwort für den Login. Beim Update mittels HTTP-Protokoll ist eine Angabe des Logins u.U. nicht erforderlich.

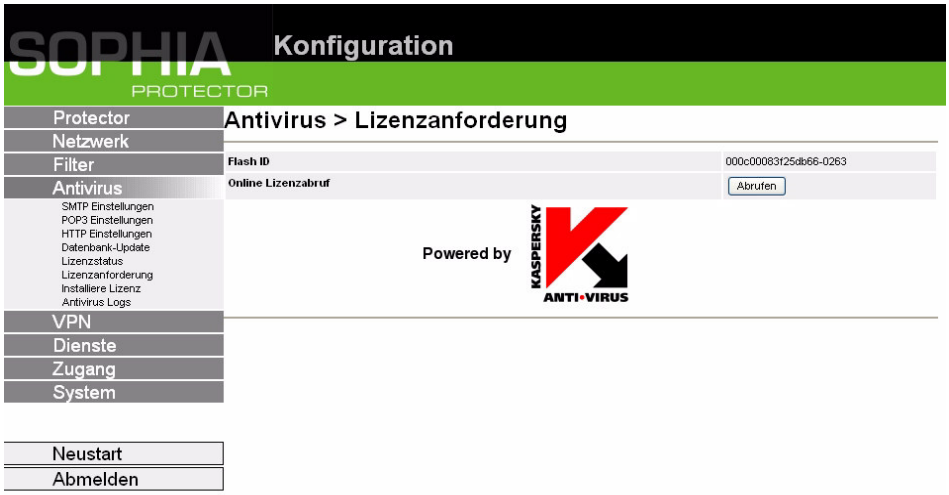
Antivirus → Lizenzstatus

Sie können die erfolgreiche Freischaltung des Virenfilters überprüfen. Unter diesem Menüpunkt finden Sie auch Informationen über das Ablaufdatum Ihrer Lizenz.



Antivirus → Lizenzanforderung

Beim Kauf Ihrer Antivirus-Lizenz erhalten Sie einen Voucher, auf dem Sie ein Lizenz-Key und eine Lizenznummer finden. Um Ihren Virenfilter zu aktivieren, müssen Sie zunächst mit diesen Informationen Ihre Lizenzdatei anfordern. Dazu drücken Sie Abrufen im Menü **Antivirus->Lizenzanforderung**.



Sie gelangen dann auf eine Web-Seite, in deren Felder Sie die folgenden Informationen eingeben:

License Serial: Die Seriennummer, die auf Ihrem Vocher gedruckt ist

License Key: Der Lizenz-Key auf Ihrem Voucher

Flash Id: Wird automatisch vorausgefüllt

Email Address: Ihre E-Mail-Adresse für die Zustellung der Lizenzdatei

Nach erfolgreichem Ausfüllen des Formulars wird Ihnen die Lizenzdatei zugesendet.

Lizenzdatei installieren

Um die Lizendatei zu installieren, wählen Sie bitte die Datei im Menüpunkt **Features->Installiere Lizenz** aus, um sie anschließend zu installieren.

Antivirus → Antivirus Logs

Das Antivirus-Log enthält folgende Meldungen des Virenfilters:

- Gefundene Viren mit Angabe von Details (Name des Virus, Name der Datei, bei einer E-Mail zusätzlich: Absender, Datum, Betreff)
- Warnungen bei automatischer Einschaltung des Durchlaßmodus, wenn die zu filternde Datei die eingestellte Dateigröße überschreitet und nicht gefiltert wurde.
- Programmstart und -ende
- Start und Verlauf des Update-Prozesses der Virensignaturdatei
- Fehlerausgaben der Kaspersky-Scan-Engine und des Virenfilters

Fehlermeldungen

Virus Detection

Ein Virus wurde erkannt. Die Fehlermeldung umfaßt den Namen des Virus, den Absender der E-Mail, das Absendedatum und den Namen der infizierten Datei bzw. den Namen der komprimierten Archivdatei und des infizierten Bestandteils dieses Archivs.

Beispiel einer Virenmeldung:

```
Innominate mGuard: Virus detection
found Virus I-Worm.NetSky.q /
[From clacla@rtfm.demon.uk]
[Date Sat, 31 Jul 2004 23:21:08 -0700]/
document_all.zip/details.txt .pif
```

Erläuterung:
Virus Name: I-Worm.NetSky.q
Absender: clacla@rtfm.demon.uk
Datum: Sat, 31 Jul 2004 23:21:08
Archivdatei: "document_all.zip"
infizierte Datei: "details.txt .pif"

Exceeded maximum filesize

Die eingestellte Begrenzung der Dateigröße wurde überschritten.
Um die Datei trotzdem übertragen zu können, deaktivieren Sie für den Download den Virenfilter für den entsprechenden Server oder global. Alternativ können Sie den Durchlaßmodus (Menüpunkt: „bei Überschreiten der Größenbegrenzung) im jeweiligen Protokoll aktivieren.

⌦ In beiden Fällen wird die übertragene Datei nicht nach Viren untersucht !

Temporary Virus Scanner Failure

Ein temporärer Fehler trat bei dem Versuch auf, eine Datei zu scannen. Eine Wiederholung der Übertragung zu einem späteren Zeitpunkt oder ein Update der Virensignaturdatei kann evtl. das Problem beheben.
Mögliche Fehlerursachen:

- Die Scan-Engine ist nicht in der Lage, die Datei zu bearbeiten
- Die Speicherkapazität des SOPHIA Protector reicht nicht zur Dekompression der Datei aus
- Interner Fehler der Scan-Engine

Exceptional Virus Scanner Failure

Ein Kommunikationproblem mit der Kaspersky-Scan-Engine trat auf. Genauere Angaben zum Problem finden Sie im Antivirus-Log.

Mögliche Fehlerursachen:

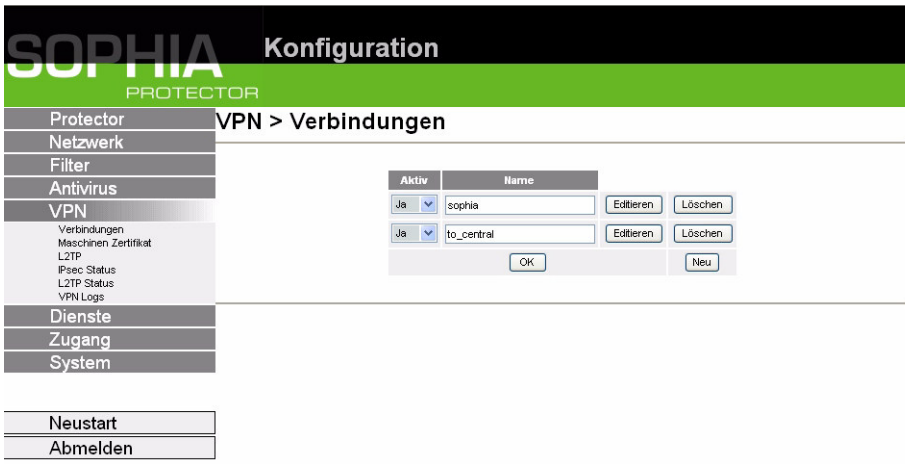
- Fehlgeschlagenes Signatur-Update durch fehlerhafte Angabe des Update-Servers (Menüpunkt Antivirus->Database Update)
- Ungültige oder veraltete Lizenz für den Virenfilter
- Beschädigtes oder fehlerhaftes Update der Virensignaturdatei

5.8 Menü VPN

Voraussetzungen für eine VPN-Verbindung:
Generelle Voraussetzung für eine VPN-Verbindung ist, dass die IP-Adressen der VPN-Partner bekannt und zugänglich sind. Siehe dazu „DynDNS-Service” auf Seite 7.

- Damit eine IPsec-Verbindung erfolgreich aufgebaut werden kann, muss die VPN-Gegenstelle IPsec mit folgender Konfiguration unterstützen:
  – Authentifizierung über Pre-Shared Key (PSK) oder X.509 Zertifikate
  – ESP
  – Diffie-Hellman Gruppe 2 oder 5
  – DES, 3DES oder AES encryption
  – MD5 oder SHA-1 Hash Algorithmen
  – Tunnel oder Transport Modus
  – Quick Mode
  – Main Mode
  – SA Lifetime (1 Sekunde bis 24 Stunden)
  Ist die Gegenstelle ein Rechner unter Windows 2000, muss dazu das *Microsoft Windows 2000 High Encryption Pack* oder mindestens das *Service Pack 2* installiert sein.
- Befindet sich die Gegenstelle hinter einem NAT-Router, so muss die Gegenstelle NAT-T unterstützen. Oder aber der NAT-Router muss das IPsec-Protokoll kennen (IPsec/VPN Passthrough). In beiden Fällen sind aus technischen Gründen nur IPsec Tunnel-Verbindungen möglich.

VPN → Verbindungen



Listet die eingerichteten VPN-Verbindungen auf.

☞ Sie können jede einzelne Verbindung aktivieren (Aktiv = **Ja**) oder deaktivieren (Aktiv = **Nein**).

VPN-Verbindung löschen

☞ Klicken Sie neben dem betreffenden Eintrag **Löschen**.
Klicken Sie abschließend **OK**.

Neue VPN-Verbindung einrichten

☞ Klicken Sie **Neu**.
Geben Sie der Verbindung einen Namen und klicken Sie **Editieren.**
Machen Sie die gewünschten bzw. erforderlichen Einstellungen (s. u.).
Klicken Sie abschließend **OK**.

VPN-Verbindung bearbeiten

☞ Klicken Sie neben der betreffenden Verbindung die Schaltfläche **Editieren**.
Machen Sie die gewünschten bzw. erforderlichen Einstellungen (s. u.).
Klicken Sie abschließend **OK**.

Ein beliebiger Name für die VPN Verbindung

Sie können die Verbindung frei benennen bzw. umbenennen.

Aktiv

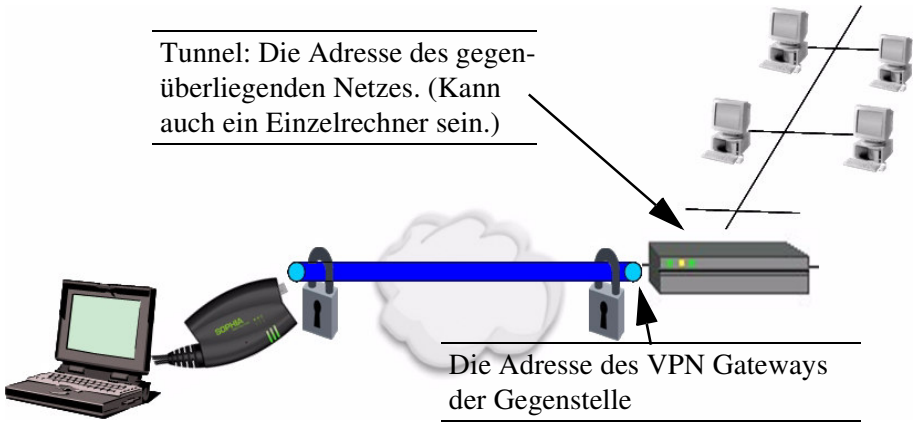
Legen Sie fest, ob die Verbindung aktiv (= Ja) sein soll oder nicht (= Nein).

Adresse des VPN Gateways der Gegenstelle

- Gemeint ist die Adresse des Übergangs zum privaten Netz, in dem sich der entfernte Kommunikationspartner befindet - siehe Abbildung unten.
- Falls der Protector aktiv die Verbindung zur entfernten Gegenstelle initiieren und aufbauen soll oder sich im *Stealth*-Modus befindet, dann geben Sie hier die IP-Adresse der Gegenstelle an. Statt einer IP-Adresse können Sie auch einen Hostnamen (d. h. Domain Namen im URL-Format in der Form www.xyz.de) eingeben.
  Falls der VPN Gateway der Gegenstelle keine feste und bekannte IP-Adresse hat, kann über die Inanspruchname des DynDNS-Service dennoch eine feste und bekannte Adresse simuliert werden. Siehe „DynDNS-Service” auf Seite 7.
- Falls der Protector bereit sein soll, die Verbindung anzunehmen, die eine entfernte Gegenstelle mit beliebiger IP-Adresse aktiv zum lokalen Protector initiiert und aufbaut, dann geben Sie an: **%any**
  Dann kann eine entfernte Gegenstelle den lokalen Protector „anrufen“, die ihre eigene IP-Adresse (vom Internet Service Provider) dynamisch zugewie-

sen erhält, d. h. eine wechselnde IP-Adresse hat. Nur wenn in diesem Szenario die entfernte „anrufende“ Gegenstelle auch eine feste und bekannte IP-Adresse hat, können Sie diese IP-Adresse angeben.

Geräte und Adressen der Gegenstelle



Verbindungstyp

Es stehen zur Auswahl:

Tunnel (Netz ←→ Netz)
Transport (Host ←→ Host)
Transport (L2TP Microsoft Windows)
Transport (L2TP SSH Sentinel)

Tunnel (Netz ←→ Netz)

Dieser Verbindungstyp eignet sich in jedem Fall und ist der sicherste. In diesem Modus werden die zu übertragenen IP-Datagramme vollkommen verschlüsselt und mit einem neuen Header versehen zur VPN-Gateway der Gegenstelle, dem „Tunnelende“, gesendet. Dort werden die übertragenen Datagramme entschlüsselt und aus ihnen die ursprünglichen Datagramme wiederhergestellt. Diese werden dann zum Zielrechner weitergeleitet.

Transport (Host ←→ Host)

Bei diesem Verbindungstyp werden nur die Daten der IP-Pakete verschlüsselt. Die IP Header Informationen bleiben unverschlüsselt.

Transport (L2TP Microsoft Windows)

Ist beim entfernten Rechner dieser Verbindungstyp aktiviert, dann setzen Sie den Protector auch auf *Transport (L2TP Microsoft Windows)*. Dann arbeitet der Protector entsprechend. Das heißt, innerhalb der IPsec-Transport-Verbindung schafft das L2TP/PPP Protokoll einen Tunnel. Dem lokal angeschlossenen L2TP-Rechner wird seine IP-Adresse vom Protector dynamisch zugewiesen.

Bei Auswahl des Verbindungstyps *Transport (L2TP Microsoft Windows)* setzen Sie *Perfect Forward Secrecy (PFS)* auf **Nein** (siehe unten). Aktivieren Sie auch den L2TP-Server.

⌦ Sobald unter Windows die IPsec/L2TP-Verbindung gestartet wird, erscheint ein Dialogfeld, das nach Benutzername und Login fragt. Sie können dort beliebige Einträge machen, denn die Authentifizierung erfolgt bereits über die X.509 Zertifikate, so dass der Protector diese Eingaben ignoriert.

Transport (L2TP SSH Sentinel)

Ist beim lokal angeschlossenen Rechner dieser Verbindungstyp aktiviert, dann setzen Sie den Protector auch auf *Transport (L2TP SSH Sentinel)*. Dann arbeitet der Protector entsprechend. Das heißt, innerhalb der IPsec-Transport-Verbindung schafft das L2TP/PPP Protokoll einen Tunnel. Dem lokal angeschlossenen L2PT-Rechner wird seine IP-Adresse vom Protector dynamisch zugewiesen. Aktivieren Sie auch den L2TP-Server.

Verbindungsinitiierung

Es gibt 2 Möglichkeiten:

- Starte die Verbindung zur Gegenstelle
- Warte auf Gegenstelle

Starte die Verbindung zur Gegenstelle

In diesem Fall initiiert der lokale Protector die Verbindung zur Gegenstelle. Im Feld *Adresse des VPN Gateways der Gegenstelle* (s. o.) muss die feste IP-Adresse der Gegenstelle oder deren Domain Namen eingetragen sein.

Warte auf Gegenstelle

In diesem Fall ist der lokale Protector bereit, die Verbindung anzunehmen, die eine entfernte Gegenstelle aktiv zum lokalen Protector initiiert und aufbaut. Im Feld *Adresse des VPN Gateways der Gegenstelle* (s. o.) kann eingetragen sein: **%any**

Baut ausschließlich eine bestimmte Gegenstelle mit fester IP-Adresse die Verbindung auf, können Sie sicherheitshalber deren IP-Adresse oder Hostnamen angeben.

⌦ Arbeitet der Protector im *Stealth*-Modus, ist diese Einstellung wirkungslos. D. h. sie wird ignoriert und die Verbindung wird automatisch initiiert, wenn der Protector bemerkt, dass die Verbindung genutzt werden soll.

Authentisierungsverfahren

Es gibt 2 Möglichkeiten:

- X.509 Zertifikat
- Pre-Shared Key

X.509 Zertifikat

Dieses Verfahren wird von den meisten neueren IPsec-Implementierungen unterstützt. Dabei verschlüsselt der Protector die Authentifizierungs-Datagramme, die es zur Gegenstelle, dem „Tunnelende“ sendet, mit dem öffentlichen Schlüssel (Dateiname *.cer oder *.pem) der Gegenstelle. (Diese *.cer- oder *.pem-Datei haben Sie vom Bediener der Gegenstelle erhalten, z. B. per Diskette oder per E-Mail).

Um diesen öffentlichen Schlüssel dem Protector zur Verfügung zu stellen, gehen Sie wie folgt vor:

Voraussetzung:

Sie haben die *.cer- oder *.pem-Datei auf dem Rechner gespeichert.

1. **Konfigurieren** klicken.
   Folge: Der Bildschirm *VPN* > *Verbindungen* > *Verbindung xyz* > *X.509 Zertifikat* erscheint. („*xyz*“ ist der jeweilige Name der Verbindung.)
2. **Durchsuchen...** klicken und die Datei selektieren.
3. **Importiere** klicken.

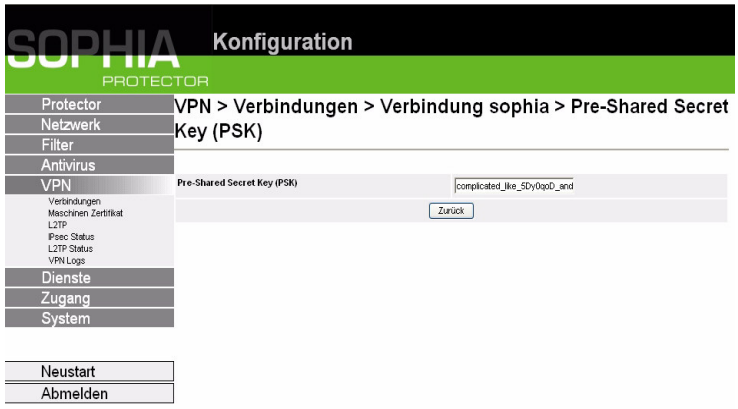
Nach dem Import wird der Inhalt des neuen Zertifikats angezeigt - siehe nachfolgende Abbildung. Eine Erläuterung der angezeigten Informationen finden Sie im Kapitel „VPN → Maschinenzertifikat” auf Seite 56.

Pre-Shared Secret Key (PSK)

Dieses Verfahren wird vor allem durch ältere IPsec Implementierungen unterstützt. Dabei verschlüsselt der Protector die Datagramme, die er zur Gegenstelle, dem „Tunnelende“ sendet, mit dem öffentlichen Schlüssel der Gegenstelle (Dateiname *.cer oder *.pem).

Um den verabredeten Schlüssel dem Protector zur Verfügung zu stellen, gehen Sie wie folgt vor:

1. **Konfigurieren** klicken.
   Folge: Der nachfolgend abgebildete Bildschirm erscheint.



2. Ins Eingabefeld *Pre-Shared Secret Key (PSK)* die verabredete Zeichenfolge eintragen. Um eine mit 3DES vergleichbare Sicherheit zu erzielen, sollte die Zeichenfolge aus ca. 30 nach dem Zufallsprinzip ausgewählten Klein- und Großbuchstaben sowie Ziffern bestehen.
3. **Zurück** klicken.

⌦ *Pre-Shared Secret Key* kann nicht mit dynamischen (%any) IP-Adressen verwendet werden, nur feste IP-Adressen oder Hostnamen auf beiden Seiten werden unterstützt.

ISAKMP SA (Schlüsselaustausch)

Verschlüsselungsalgorithmus

☞ Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verschlüsselungsverfahren verwendet werden soll.

3DES-168 ist das am häufigsten benutzte Verfahren und ist deshalb als Standard voreingestellt.

Grundsätzlich gilt Folgendes: Je mehr Bits ein Verschlüsselungsalgorithmus hat - angegeben durch die angefügte Zahl -, desto sicherer ist er. Das relativ neue Verfahren AES-256 gilt daher als am sichersten, ist aber noch nicht so verbreitet.

Der Verschlüsselungsvorgang ist um so zeitaufwendiger, je länger der Schlüssel ist. Dieser Gesichtspunkt spielt für den Protector keine Rolle, weil er mit Hardware-basierter Verschlüsselungstechnik arbeitet. Jedoch könnte dieser Aspekt für die Gegenstelle eine Rolle spielen.

Der zur Auswahl stehende mit „Null“ bezeichnete Algorithmus beinhaltet keinerlei Verschlüsselung.

Prüfsummenalgorithmus/Hash

Lassen Sie die Einstellung auf *Alle Algorithmen* stehen. Dann spielt es keine Rolle, ob die Gegenstelle mit MD5 oder SHA-1 arbeitet.

IPsec SA (Datenaustausch)

Im Unterschied zu *ISAKMP SA (Schlüsselaustausch)* (s. o.) wird hier das Verfahren für den Datenaustausch festgelegt. Die können sich von denen des Schlüsselaustauschs unterscheiden, müssen aber nicht.

Verschlüsselungsalgorithmus

Siehe oben.

Prüfsummenalgorithmus/Hash

Siehe oben.

Perfect Forward Secrecy (PFS)

Verfahren zur zusätzlichen Steigerung der Sicherheit bei der Datenübertragung. Bei IPsec werden in bestimmten Intervallen die Schlüssel für den Datenaustausch erneuert. Mit PFS werden dabei mit der Gegenstelle neue Zufallszahlen ausgehandelt, anstatt sie aus zuvor verabredeten Zufallszahlen abzuleiten.

☞ Nur wenn die Gegenstelle PFS unterstützt, wählen Sie **Ja**.

Bei Auswahl des Verbindungstyps *Transport (L2TP Microsoft Windows)* setzen Sie *Perfect Forward Secrecy (PFS)* auf **Nein**.

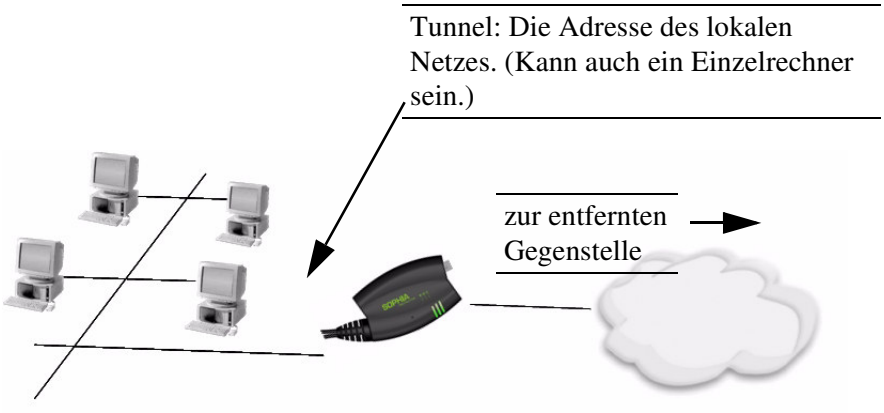
Tunnel Einstellungen

Die Adresse des lokalen Netzes

Die dazugehörige Netzmaske

Mit diesen beiden Angaben geben Sie die Adresse des Clients (Netz oder Rechner) an, der lokal direkt am Protector direkt angeschlossen ist und den der Protector schützt. Diese Adresse bezeichnet den lokalen Endpunkt der Verbindung.

Lokale Geräte und Adressen



Beispiel:

Ist am Protector der Rechner angeschlossen, den Sie auch zur Konfiguration des Gerätes benutzen, dann könnten diese Angaben lauten:

Adresse des lokalen Netzes: 192.168.1.1

Die dazugehörige Netzmaske: 255.255.255.0

Siehe auch „Netzwerk-Beispielskizze” auf Seite 78.

Die virtuelle IP für den Client im Stealth Modus

Ein VPN-Tunnel kann nur zwei lokale Netzwerke über ein öffentliches Netz miteinander verbinden. Arbeitet der Protector im *Stealth*-Modus, dann ist an ihm aber nur ein Einzelrechner angeschlossen - siehe „Netzwerk → Stealth” auf Seite 25. Zum Aufbau des VPN-Tunnels muss darum ein angeschlossenes lokales Netz simuliert werden. In diesem erhält der am Protector angeschlossene Rechner eine virtuelle IP-Adresse.

Diese virtuelle IP-Adresse ist für die entfernte Gegenstelle die Adresse des (simulierten) lokalen Netzes, unter der der real am Protector angeschlossene Rechner im VPN erreichbar ist. Für die Gegenstelle bedeutet das, dass dort diese simulierte IP-Adresse als *Adresse des gegenüberliegenden Netzes* bei der Konfiguration der VPN-Verbindung anzugeben ist.

Der lokal am Protector angeschlossene Rechner „weiß“ von dieser virtuellen IP nichts, unter der er von der Gegenseite angesprochen wird. D. h. er muss nicht konfiguriert werden.

Das bedeutet praktisch:

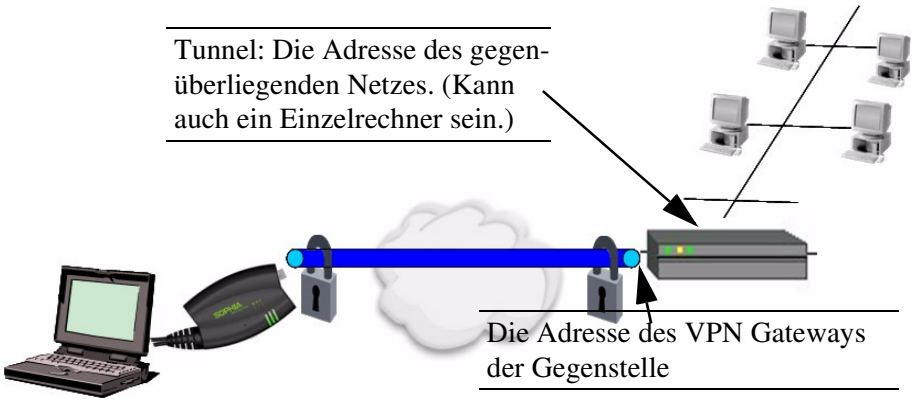
☞ Geben Sie eine beliebige IP-Adresse in der Form 192.xxx.xxx.xxx (x = eine beliebige Ziffer) an, die aber nicht auf der Gegenseite bereits vergeben sein darf. Stimmen Sie sich also mit der Gegenseite ab.
Diese virtuelle IP-Adresse ist bei der entfernten Gegensstelle bei der Konfiguration dieser VPN-Verbindung als *Adresse des gegenüberliegenden Netzes* anzugeben.

Die Adresse des gegenüberliegenden Netzes

Die dazugehörige Netzmaske

Mit diesen beiden Angaben geben Sie die Adresse des Netzes an, in dem sich der entfernte Kommunikationspartner befindet. Diese Adresse kann auch die eines Rechners sein, der direkt am VPN-Gateway angeschlossen ist.

Geräte und Adressen der Gegenstelle



.

Firewall eingehend, Firewall ausgehend

Während die unter dem Menüpunkt *Filter* vorgenommenen Einstellungen sich nur auf Nicht-VPN-Verbindungen beziehen (siehe oben unter „Filter → Eingehend" auf Seite 30), beziehen sich die Einstellungen hier ausschließlich auf die hier definierte VPN-Verbindung. Das bedeutet praktisch: Haben Sie mehrere VPN-Verbindungen definiert, können Sie für jede einzelne den Zugriff von außen oder von innen beschränken. Versuche, die Beschränkungen zu übergehen, können Sie ins Log protokollieren lassen.

⌧ Gemäß werksseitiger Voreinstellung ist die VPN-Firewall so eingestellt, dass für diese VPN-Verbindung alles zugelassen ist.
Für jede einzelne VPN-Verbindung gelten aber unabhängig voneinander gleichwohl die erweiterten Firewall-Einstellungen, die weiter oben definiert und erläutert sind - siehe „Filter → Erweiterte Einstellungen" auf Seite 34.

⌧ Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

☞ Um eine Firewall-Regel zu setzen oder zu löschen gehen Sie genauso vor wie oben beschrieben; siehe „Filter → Eingehend" auf Seite 30 und „Filter → Ausgehend" auf Seite 31.

Wie dort haben Sie bei den Angaben folgende Möglichkeiten:

- Protokoll: **Alle** bedeutet: TCP, UDP, ICMP und andere IP-Protokolle.
- IP-Adresse: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)" auf Seite 77.
- Port: (wird nur ausgewertet bei den Protokollen TCP und UDP)
  any bezeichnet jeden beliebigen Port.
  startport:endport (z. B. 110:120) bezeichnet einen Portbereich.
  Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

- Aktion:
  Annehmen bedeutet, die Datenpakete dürfen passieren.
  Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat Abweisen dieselbe Wirkung wie Verwerfen (s. u.).)
  Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

Log
Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

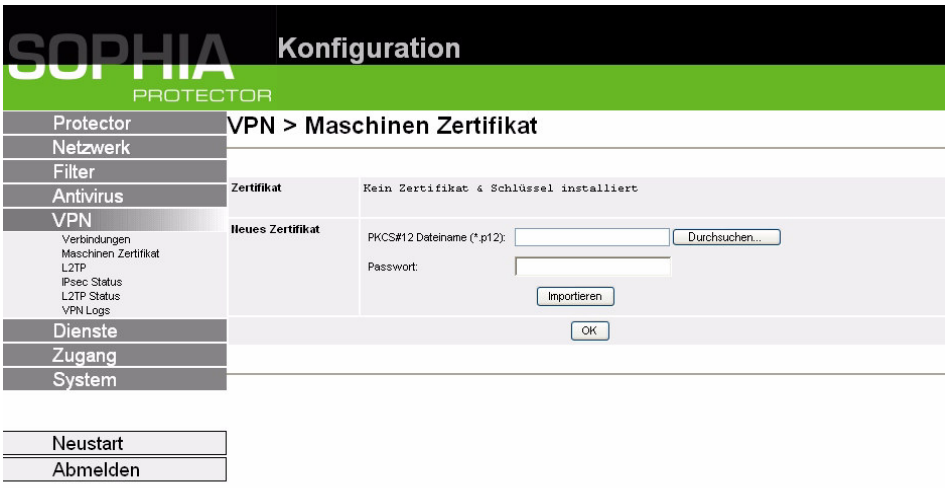
☞ das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen

☞ oder nicht - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

Log-Einträge für unbekannte Verbindungsversuche
Damit werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.

⌦ Im Stealth-Modus ist **Abweisen** als Aktion nicht möglich.
⌦ Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge befolgt.

VPN → Maschinenzertifikat



Zertifikat
Zeigt das aktuell importierte X.509-Zertifikat an, mit dem sich der Protector gegenüber anderen VPN-Gateways ausweist. Folgende Informationen werden angezeigt:

subject	Der Besitzer, auf den das Zertifikat ausgestellt ist.
issuer	Die Beglaubigungsstelle, die das Zertifikat unterschrieben hat. C : Land (Country) ST: Bundesland (State) L : Stadt (Location) O : Organisation OU: Abteilung (Organisation Unit) CN: Hostname, allgemeiner Name (Common Name)

MD5, SHA1 Fingerprint	Fingerabdruck des Zertifikats, um diesen z. B. am Telefon mit einem anderen zu vergleichen. Windows zeigt an dieser Stelle den Fingerabdruck im SHA1-Format an.
notBefore, notAfter	Gültigkeitszeitraum des Zertifikats. Wird vom Protector magels einer eingebauten Uhr ignoriert.

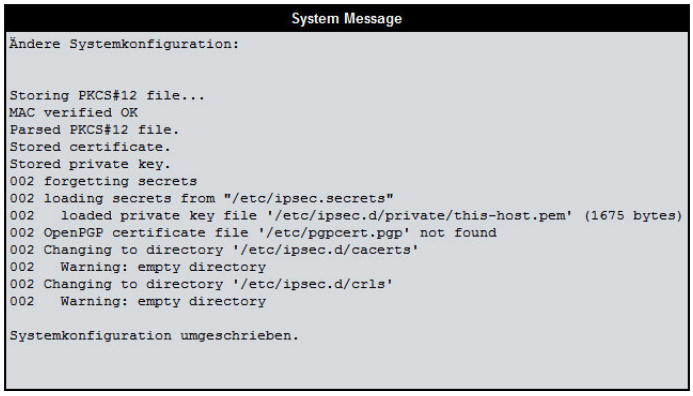
Die importierte Zertifikatsdatei (Dateinamen-Erweiterung *.p12 oder *.pfx) enthält neben den oben angegebenen Informationen die beiden Schlüssel, den öffentlichen zum Verschlüsseln, den privaten zum Entschlüsseln. Der zugehörige öffentliche Schlüssel kann an beliebig viele Verbindungspartner vergeben werden, so dass diese verschlüsselte Daten senden können.
In Abhängigkeit von der Gegenstelle muss das Zertifikat als .cer- oder .pem-Datei dem Bediener der entfernten Gegenstelle zur Verfügung gestellt werden - z. B. durch persönliche Übergabe oder per E-Mail. Wenn Ihnen kein sicherer Übertragungsweg zur Verfügung steht, sollten Sie anschließend den vom mGaurd angezeigten Fingerabdruck über einen sicheren Weg vergleichen.

Es kann nur eine Zertifikats-Datei (PKCS#12-Datei) ins Gerät importiert werden.
Um ein (neues) Zertifikat zu importieren, gehen Sie wie folgt vor:

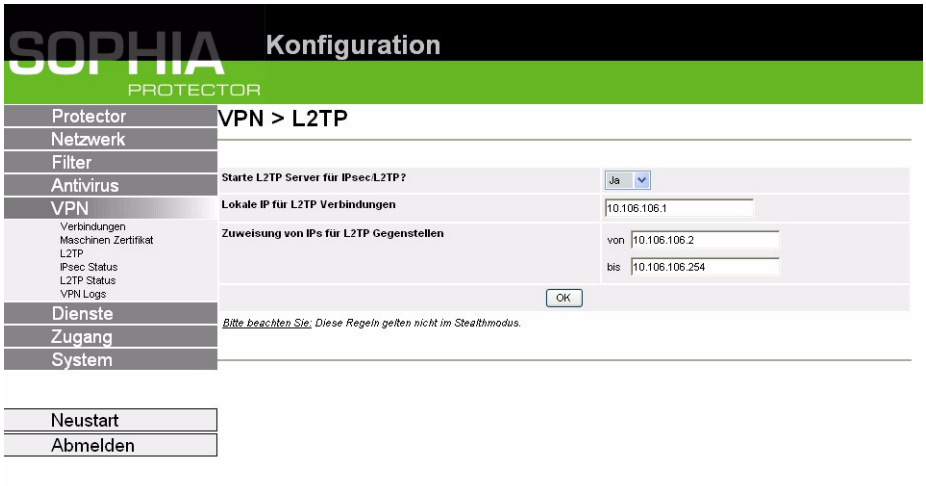
Neues Zertifikat

Voraussetzung:
Die Zertifikatsdatei (Dateiname = *.p12 oder *.pfx) ist generiert und auf dem angeschlossenen Rechner gespeichert.

1. **Durchsuchen...** klicken, um die Datei zu selektieren
2. In das Feld *Passwort* geben Sie das Passwort ein, mit dem der private Schlüssel der PKCS#12-Datei geschützt ist.
3. **Importieren** klicken.
4. Abschließend **OK** klicken.
   Nach dem Import erhalten Sie eine Systemmeldung:



VPN → L2TP (nur Protector M,L)



Start L2TP Server für IPsec/L2TP? Ja / Nein

Wollen Sie eine L2TP-Verbindung ermöglichen, setzen Sie diesen Schalter auf **Ja**.

Innerhalb der IPsec Transport-Verbindung beinhaltet die L2TP Verbindung wiederum eine PPP-Verbindung. Im Ergebnis entsteht dadurch praktisch eine Art Tunnel zwischen 2 Netzen. Dabei teilt der Protector der Gegenstelle über PPP mit, welche Adressen benutzt werden: für sich selber und die entfernte Gegenstelle.

Lokale IP für L2TP Verbindungen

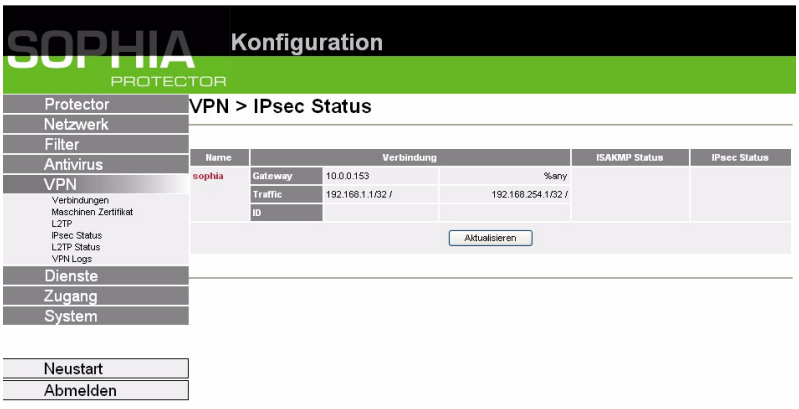
Nach dem obigen Screenshot teilt der Protector der Gegenstelle mit, er habe die Adresse 192.168.1.1.

Zuweisung von IPs für L2TP Gegenstellen

Nach dem obigen Screenshot teilt der Protector der Gegenstelle mit, diese habe die Adressen ab 10.106.106.2 (bei einem einzigen Rechner) bis 10.106.106.254 (bei mehreren Rechnern).

VPN → IPsec Status

Nur Anzeige



Informiert über den Status der IPsec-Verbindungen.

Links sind die Namen der VPN-Verbindungen aufgelistet, rechts daneben wird jeweils deren aktueller Status angezeigt.

GATEWAY
: bezeichnet die kommunizierenden VPN-Gateways

TRAFFIC
: bezeichnet Rechner bzw. Netze, die über die VPN-Gateways kommunizieren.

ID

bezeichnet den Distinguished Name (DN) eines X.509-Zertifikats.

ISAKMP Status

ISAKMP Status (Internet security association and key management protocol) ist mit „established“ angegeben, wenn die beiden beteiligten VPN-Gateways einen Kanal zum Schlüsselaustausch aufgebaut haben. In diesem Fall konnten sie einander kontaktieren, und alle Einträge bis einschließlich „ISAKMP SA“ auf der Konfigurationsseite der Verbindung waren korrekt.

IPsec Status

IPsec Status ist mit „established“ angegeben, wenn die IPsec-Verschlüsselung bei der Kommunikation aktiviert ist. In diesem Fall waren auch die Angaben unter „IPsec SA“ und „Tunnel-Einstellungen“ korrekt.

Bei Problemen empfiehlt es sich, in die VPN-Logs des Rechners zu schauen, zu dem die Verbindung aufgebaut wurde. Denn der initiierende Rechner bekommt aus Sicherheitsgründen keine ausführlichen Fehlermeldungen zugesandt.

Falls angezeigt wird:

ISAKMP SA established, IPsec State: WAITING

Dann bedeutet das:

Die Authentifizierung war erfolgreich, jedoch stimmten die anderen Parameter nicht: Stimmt der Verbindungstyp (Tunnel, Transport) überein? Wenn Tunnel gewählt ist, stimmen die Netzbereiche auf beiden Seiten überein?

Falls angezeigt wird:

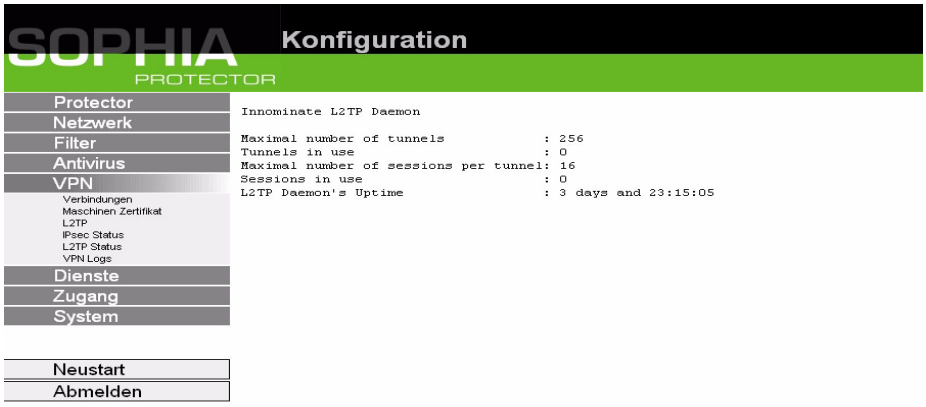
IPsec State: IPsec SA established

Dann bedeutet das:

Die VPN-Verbindung ist erfolgreich aufgebaut und kann genutzt werden. Sollte dies dennoch nicht der Fall sein, dann gibt es Probleme mit dem VPN-Gateway der Gegenstelle. In diesem Fall den Verbindungsnamen anklicken und dann **OK** klicken, um die Verbindung erneut aufzubauen.

VPN → L2TP Status

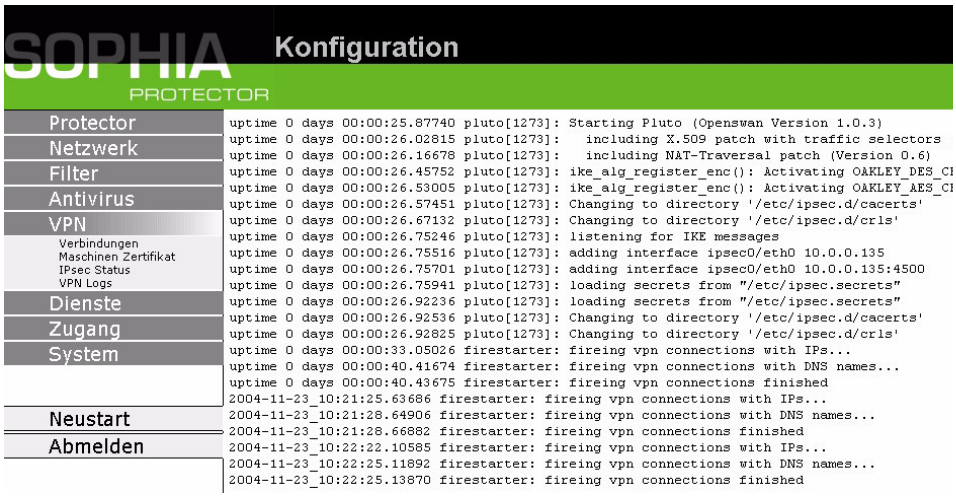
Nur Anzeige



Informiert über den L2TP-Status, wenn dieser als Verbindungstyp gewählt ist. Siehe „VPN → Verbindungen” auf Seite 48.

Ist dieser Verbindungstyp nicht gewählt, sehen Sie die abgebildete Anzeige.

VPN → VPN Logs

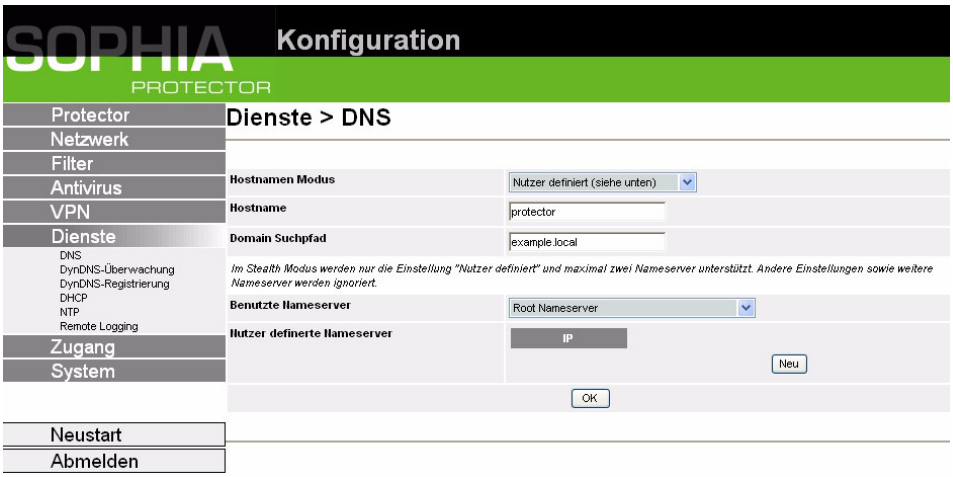


Nur Anzeige

Listet alle VPN-Ereignisse auf.
Das Format entspricht dem unter Linux gebräuchlichen Format.
Es gibt spezielle Auswertungsprogramme, die Ihnen die Informationen aus den protokollierten Daten in einem besser lesbaren Format präsentieren.

5.9 Menü Dienste

Dienste → DNS



Soll der Protector eine Verbindung zu einer Gegenstelle aufbauen (z. B. VPN-Gateway oder NTP-Server), muss ihm die IP-Adresse dieser Gegenstelle bekannt sein. Wird ihm die Adresse in Form einer Domain-Adresse angegeben (d. h. in der Form www.abc.xyz.de), dann muss das Gerät auf einem Domain Name Server (DNS) nachschlagen, welche IP-Adresse sich hinter der Domain-Adresse verbirgt.

Wenn sich der Protector nicht im *Stealth*-Modus befindet, können Sie die lokal angeschlossenen Clients so konfigurieren, dass sie den mGaurd zur Auflösung von Hostnamen in IP-Adressen benutzen können. Siehe „☞ IP-Konfiguration bei Windows-Clients” auf Seite 65

Hostnamen Modus

Mit *Hostnamen Modus* und *Hostname* können Sie dem Protector einen Namen geben. Dieser wird dann z. B. beim Einloggen per SSH angezeigt. Eine Namensgebung erleichtert die Administration mehrerer Protectors.

Nutzer definiert (siehe unten)

(Standard) Der im Feld *Hostname* eingetragene Name wird als Name für den Protector gesetzt.

⌦ Arbeitet der Protector im *Stealth*-Modus, muss als *Hostnamen Modus* die Option *Nutzer definiert* gewählt werden.

Provider definiert (z. B. via DHCP)

Wenn der Netzwerkmodus ein externes Setzen des Hostnamens erlaubt wie z. B. bei DHCP, dann wird der vom Provider übermittelte Name für den Protector gesetzt.

Hostname

Ist unter *Hostnamen Modus* die Option *Nutzer definiert* ausgewählt, dann tragen Sie hier den Namen ein, den der Protector erhalten soll.

Sonst, d. h. wenn unter *Hostnamen Modus* die Option *Provider definiert (z. B. via DHCP)* ausgewählt ist, dann wird ein Eintrag in diesem Feld ignoriert.

Domain-Suchpfad

Erleichtert dem Benutzer die Eingabe eines Domain-Namens: Gibt der Benutzer den Domain-Name gekürzt ein, ergänzt der Protector seine Eingabe um den angegebenen Domain-Suffix, der hier unter *Domain-Suchpfad* festgelegt wird.

Benutzte Nameserver

Möglichkeiten: *Root Nameserver / Provider definiert / Nutzer definiert*

Root Nameserver:
Anfragen werden an die Root-Nameserver im Internet gerichtet, deren IP-Adressen im Protector gespeichert sind. Diese Adressen ändern sich selten. Diese Einstellung sollte nur gewählt werden, wenn die alternativen Einstellungen nicht funktionieren.

Provider definiert (z. B. via PPPoE oder DHCP)
Es wird der Domain Name Server des Internet Service Providers benutzt, der den Zugang zum Internet zur Verfügung stellt. Diese Einstellung können Sie wählen, wenn der Protector im *PPPoE*-, im *PPTP*-Modus oder im *Router*-Modus arbeitet bei aktiviertem DHCP (siehe „Dienste → DHCP" auf Seite 64).

Nutzer definiert (unten stehende Liste)
Ist diese Einstellung gewählt, nimmt der Protector mit den Domain Name Servern Verbindung auf, die in der Liste *Nutzer definierte Nameserver* aufgeführt sind.
Im Stealth-Modus werden nur die 2 ersten Einträge in dieser Liste ausgewertet.

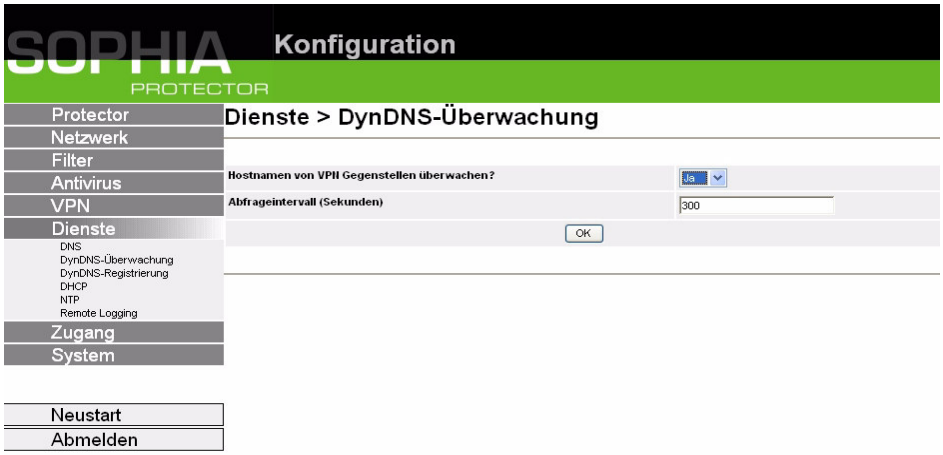
Nutzer definierter Nameserver

In dieser Liste können Sie die IP-Adressen von Domain Name Servern erfassen. Soll einer von diesen vom Protector benutzt werden, wählen Sie unter **Benutze Nameserver** die Option *Nutzer definiert (unten stehende Liste)* fest.

⌧ Wenn Sie **Nutzer definiert** eingestellt haben, müssen Sie die lokal angeschlossenen Clients so konfigurieren, dass sie die Adresse des Protector verwenden, um von ihm die Auflösung von Hostnamen in IP-Adressen zu beziehen.
Siehe „☞ IP-Konfiguration bei Windows-Clients" auf Seite 65.

Dienste → DynDNS Überwachung

Erläuterung zu DynDNS siehe unten: Dienste → DynDNS Registrierung.

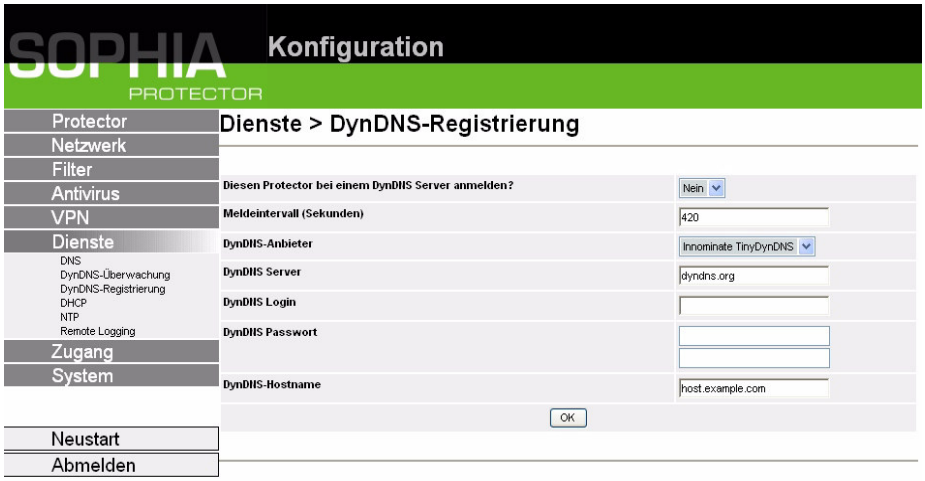


Hostnamen von VPN Gegenstellen überwachen? Ja / Nein
Ist dem Protector die Adresse der VPN-Gegenstelle als Hostname angegeben (siehe „VPN → Verbindungen" auf Seite 48), und ist dieser Domain Name von einem DynDNS Service zugeteilt, dann kann der Protector regelmäßig

überprüfen, ob beim betreffenden DynDNS keine Änderung erfolgt ist. Falls ja, wird die VPN-Verbindung zu der neuen IP-Adresse aufgebaut.

Abfrageintervall (Sekunden)
Standard: 300 (Sekunden)

Dienste → DynDNS Registrierung



Zum Aufbau von VPN-Verbindungen muss mindestens die IP-Adresse eines der Partner bekannt sein, damit diese miteinander Kontakt aufnehmen können. Diese Bedingung ist nicht erfüllt, wenn beide Teilnehmer ihre IP-Adressen dynamisch von ihrem Internet Service Provider zugewiesen bekommen. In diesem Fall kann aber ein DynDNS-Service wie z. B. DynDNS.org oder DNS4BIZ.com helfen. Bei einem DynDNS-Service wird die jeweils gültige IP-Adresse unter einem festen Namen registriert wird. Siehe auch „DynDNS-Service" auf Seite 7.
Sofern Sie für einen vom Protector unterstützten DynDNS-Service registriert sind, können Sie in diesem Dialogfeld die entsprechenden Angaben machen.

Diesen Protector bei einem DynDNS Server anmelden? Ja / Nein
Wählen Sie **Ja**, wenn Sie beim DynDNS-Anbieter entsprechend registriert sind und der Protector den Service benutzen soll. Dann meldet der Protector die aktuelle IP-Adresse, die dem eigenen Internet-Anschluss vom Internet Service Provider zugewiesen ist, an den DynDNS Service.

Meldeintervall (Sekunden)
Standard: 420 (Sekunden).
Immer wenn die IP-Adresse des eigenen Internet-Anschlusses geändert wird oder ist, informiert der Protector den DynDNS Service über die neue IP-Adresse. Aus Zuverlässigkeitsgründen erfolgt diese Meldung zusätzlich in dem hier festgelegten Zeitintervall.

DynDNS Anbieter
Die zur Auswahl gestellten Anbieter unterstützen das Protokoll, das auch der Protector unterstützt.
Geben Sie den Namen des Anbieters an, bei dem Sie registriert sind, z. B. DynDNS.org

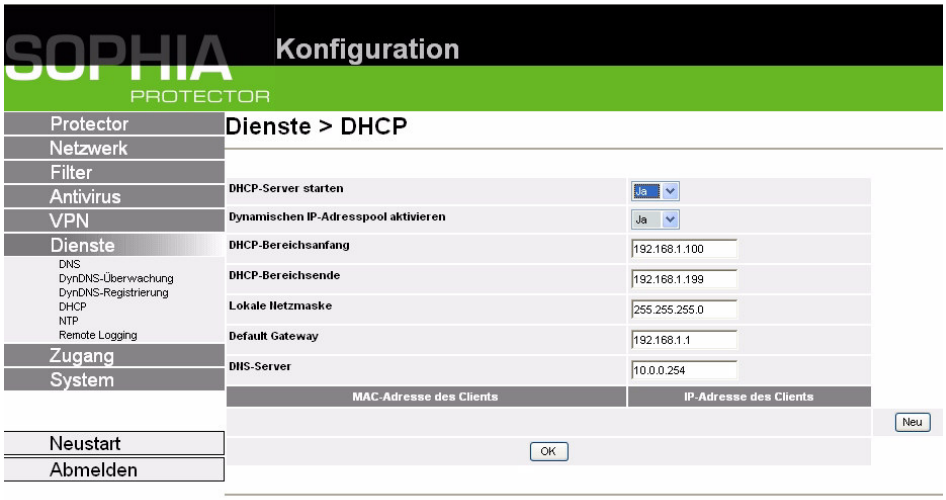
DynDNS Server
Name des Servers des oben ausgewählten DynDNS-Anbieters, z. B.: dyndns.org

DynDNS Login, DynDNS Passwort
Geben Sie hier den Benutzernamen und das Passwort ein, das Ihnen vom DynDNS-Anbieter zugeteilt worden ist.

DynDNS Hostname

Der für diesen Protector gewählte Hostname beim DynDNS-Service - sofern Sie einen DynDNS-Dienst benutzen und oben die entsprechenden Angaben gemacht haben.

Dienste → DHCP



(DHCP = Dynamic Host Configuration Protocol) Diese Funktion ordnet den lokal am Protector angeschlossenen Clients automatisch die gebotene Netzwerkkonfiguration zu (IP-Adresse und Subnetzmaske).

DHCP-Server starten

Setzen Sie diesen Schalter auf **Ja**, wenn Sie diese Funktion aktivieren wollen.

Dynamischen IP-Adresspool aktivieren

Setzen Sie diesen Schalter auf **Ja**, wenn sie den durch DHCP-Bereichsanfang bzw. DHCP-Bereichsende gewählten IP-Adresspool verwenden wollen.

Setzen Sie diesen Schalter auf **Nein**, wenn nur statische Zuweisungen anhand der MAC-Adresse vorgenommen werden sollen (siehe unten).

Optionen:

Bei aktiviertem DHCP-Server und aktiviertem dynamischem IP-Adresspool können Sie die Netzwerkparameter angeben, die vom Client benutzt werden sollen:

DHCP-Bereichsanfang: **DHCP-Bereichsende:**	Anfang und Ende des Adressbereichs, aus dem der DHCP-Server des Protector den lokal angeschlossenen Clients IP-Adressen-zuweisen soll.
Lokale Netzmaske:	Voreingestellt ist: 255.255.255.0
Default-Gateway:	Legt fest, welche IP-Adresse beim Client als Standardgateway benutzt wird. In der Regel ist das die lokale IP-Adresse des Protector.

DNS-Server: Legt fest, von wo Clients die Auflösung von Hostnamen in IP-Adressen beziehen. Wenn der DNS-Dienst des Protector aktiviert ist, kann das die lokale IP-Adresse des Protector sein.

Statische Zuweisungen anhand der MAC-Adresse

Die MAC-Adresse Ihres Clients finden Sie wie folgt heraus:
Windows 95/98/ME: Starten Sie "winipcfg" in einer DOS-Box Windows **NT/2000/XP**: Starten Sie "ipconfig /all" in einer Eingabeaufforderung. Die MAC-Adresse wird als "Physikalische Adresse" angezeigt.
Linux: Rufen sie in einer Shell "/sbin/ifconfig" oder "ip link show" auf .

Zuweisung löschen

☞ Klicken Sie neben dem betreffenden Eintrag **Löschen**, dann **OK**.

Zuweisung hinzufügen

☞ Wollen Sie eine neuen Zuweisung hinzufügen, klicken Sie **Neu**.
Geben Sie die Daten der Zuweisung an (s. u.) und klicken Sie **OK**.

Bei den Angaben haben Sie folgende Möglichkeiten:

MAC-Adresse des Clients
Die MAC-Adresse (ohne Leerzeichen oder Bindestriche) des Clients.

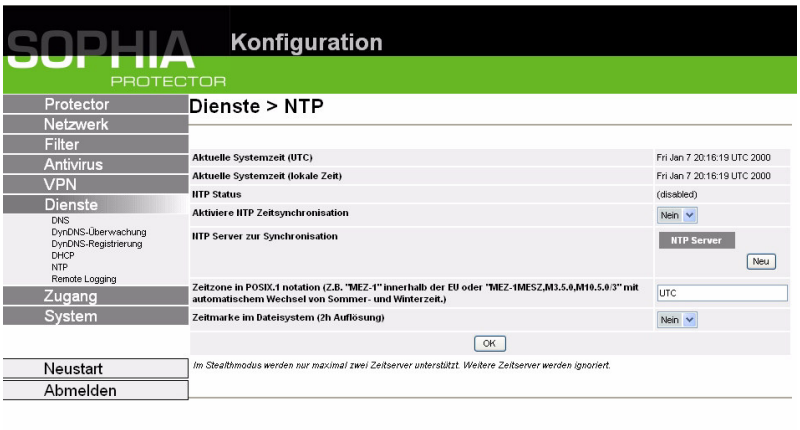
IP-Adresse des Clients
Die statische IP des Clients, die der MAC-Adresse zugewiesen werden soll.

⌧ Die statischen Zuweisungen haben Vorrang vor dem dynamischen IP-Adresspool.
⌧ Statische Zuweisungen dürfen sich nicht mit dem dynamischen IP-Adresspool überlappen.
⌧ Eine IP darf nicht in mehreren statischen Zuweisungen verwendet werden, ansonsten wird diese IP mehreren MAC-Adressen zugeordnet.
⌧ Es darf nur ein DHCP-Server pro Subnetz verwendet werden.
⌧ Wenn Sie den DHCP-Server des Protector starten, müssen Sie die lokal angeschlossenen Clients so konfigurieren, dass sie ihre IP-Adressen automatisch beziehen (s. u.).

☞ **IP-Konfiguration bei Windows-Clients**

Dazu klicken Sie unter Windows XP **Start->Systemsteuerung->Netzwerkverbindungen**: Symbol des LAN-Adapters mit der rechten Maustaste klikken und im Kontextmenü **Eigenschaften** klicken. Im Dialogfeld *Eigenschatten von LAN-Verbindung* lokales Netz auf der Registerkarte *Allgemein* unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag **Internetprotokoll (TCP/IP)** markieren und dann die Schaltfläche **Eigenschaften** klikken.
Im Dialogfeld *Eigenschaften von Internetprotokoll (TCP/IP)* die gebotenen Angaben bzw. Einstellungen machen.

Dienste → NTP



(NTP = Network Time Protokoll)

Aktuelle Systemzeit (UTC)

Anzeige der aktuellen Systemzeit in Universal Time Coordinates (UTC). Wenn die *NTP Zeitsynchronisation* noch nicht aktiviert ist (s. u.), und *Zeitmarken im Dateisystem* deaktiviert sind, beginnt die Uhr mit dem 1. Januar 2000.

Aktuelle Systemzeit (lokale Zeit)

Soll die eventuell abweichende aktuelle Ortszeit angezeigt werden, müssen Sie unter *Zeitzone in POSIX.1 Notation...* (s. u.) den entsprechenden Eintrag machen.

NTP Status

Anzeige des aktuellen NTP-Status

Aktiviere NTP Zeitsynchronisation: Ja / Nein

Sobald das NTP aktiviert ist, bezieht der Protector die Zeit aus dem Internet und zeigt diese als aktuelle Systemzeit an. Die Synchronisation kann einige Sekunden dauern.

Nur wenn dieser Schalter auf **Ja** steht und unter *NTP Server zur Synchronisation* (s. u.) mindestens 1 Zeitserver angegeben ist, wird die aktuelle Systemzeit zur Verfügung gestellt.

NTP Server zur Synchronisation

Geben Sie hier einen oder mehrere Zeitserver an, von denen der Protector die aktuelle Zeitangabe beziehen soll. Falls Sie mehrere Zeitserver angeben, verbindet sich der Protector automatisch mit allen, um die aktuelle Zeit zu ermitteln.

- Wenn Sie statt einer IP-Adresse einen Hostnamen, z. B. pool.ntp.org, angeben, muss ein DNS-Server festgelegt sein - siehe „Dienste → DNS" auf Seite 61.
- Arbeitet der Protector im *Stealth*-Modus und sind mehrere Zeitserver angegeben, werden nur die ersten beiden Zeitserver in der Liste benutzt.
- Arbeitet der Protector im *Router- PPPoE-* oder *PPTP*-Modus, stellt er auch den angeschlossenen Rechnern die NTP-Zeit zur Verfügung.

Zeitzone in POSIX.1 Notation...

Soll oben unter *Aktuelle Systemzeit* nicht die aktuelle Greenwich-Zeit angezeigt werden sondern Ihre aktuelle Ortszeit (= abweichend von der Greenwich-Zeit), dann tragen Sie hier ein, um wieviel Stunden bei Ihnen die Zeit voraus bzw. zurück ist.

Beispiele:

In Berlin ist die Uhrzeit der Greenwich-Zeit um 1 Stunde voraus. Also tragen Sie ein: MEZ-1

Wichtig ist allein die Angabe -1, -2 oder +1 usw., weil nur sie ausgewertet wird; die davor stehenden Buchstaben nicht. Sie können „MEZ" oder beliebig anders lauten.

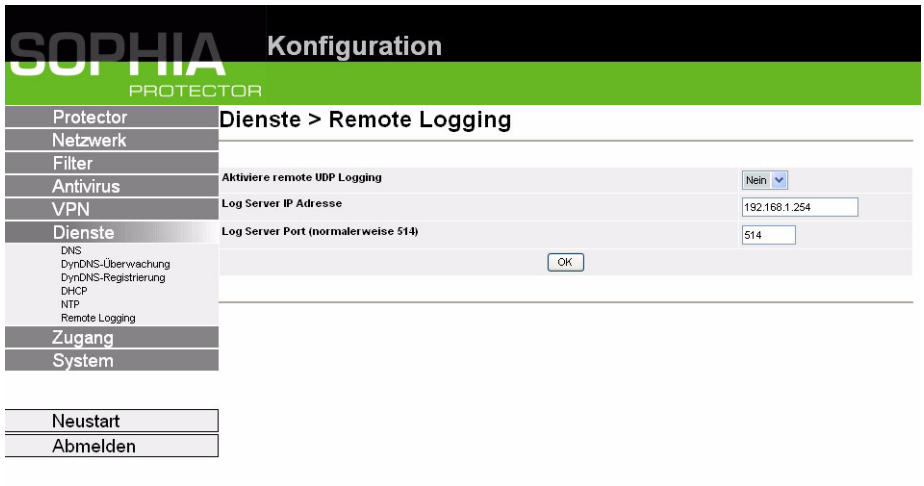
Wünschen Sie die Anzeige der MEZ-Uhrzeit (= gültig für Deutschland) mit automatischer Umschaltung auf Sommer- bzw. Winterzeit geben Sie ein:
MEZ-1MESZ,M3.5.0,M10.5.0/3

Zeitmarke im Dateisystem (2h Auflösung): Ja / Nein

Ist dieser Schalter auf **Ja** gesetzt, schreibt der Protector alle 2 Stunden die aktuelle Systemzeit in seinen Speicher.

Folge: Wird der Protector aus- und wieder eingeschaltet, wird nach dem Einschalten eine Uhrzeit in diesem 2-Stunden-Zeitfenster angezeigt und nicht eine Uhrzeit am 1. Januar 2000.

Dienste → Remote Logging (nur Protector M,L)



Alle Log-Einträge finden standardmäßig im Arbeitsspeicher des Protector statt. Ist der maximale Speicherplatz für diese Protokollierungen erschöpft, werden automatisch die ältesten Log-Einträge durch neue überschrieben. Zudem werden bei Ausschalten des Protector alle Log-Einträge gelöscht.

Um das zu verhindern, ist es möglich, die Log-Einträge auf einen externen Rechner zu übertragen. Das liegt auch dann nahe, soll eine zentrale Verwaltung der Protokollierungen erfolgen.

Aktiviere remote UDP Logging: Ja / Nein

Sollen alle Log-Einträge zum externen (unten angegebenen) Log Server übertragen werden, setzen Sie diesen Schalter auf **Ja**.

Log Server IP Adresse

Geben Sie die IP-Adresse des Log Servers an, zu dem die Log-Einträge per UDP übertragen werden sollen.

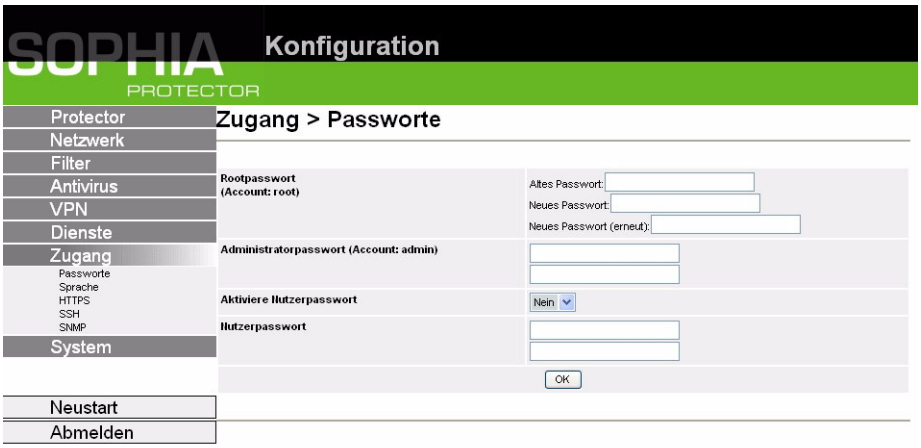
⌦ Sie müssen eine IP-Adresse angeben, keinen Hostnamen! Hier wird eine Namensauflösung nicht unterstützt, weil sonst der Ausfall eines DNS-Servers nicht protokolliert werden könnte.

Log Server Port

Geben Sie den Port des Log Servers an, zu dem die Log-Einträge per UDP übertragen werden sollen. Standard: 514

5.10 Menü Zugang

Zugang → Passworte



Der Protector bietet 3 Stufen von Benutzerrechten. Um sich auf der entsprechenden Stufe anzumelden, muss der Benutzer das Passwort angeben, dass der jeweiligen Berechtigungsstufe zugeordnet ist.

Berechtigungsstufe	
Root	Bietet vollständige Rechte für alle Parameter des Protector. Hintergrund: Nur diese Berechtigungsstufe erlaubt es, sich per SSH so mit dem Gerät zu verbinden, dass man das ganze System auf den Kopf stellen kann. Dann kann man es nur noch mit „Flashen“ der Firmware in seinen Auslieferungszustand zurückbringen (siehe „Flashen der Firmware” auf Seite 80). Voreingestelltes Rootpasswort: **root**
Administrator	Bietet die Rechte für die Konfigurationsoptionen, die über die webbasierte Administratoroberfläche zugänglich sind. Voreingestellter Benutzername: **admin** Voreingestelltes Passwort: **Protector** Der Benutzername **admin** kann nicht geändert werden.
Nutzer	Ist ein Nutzerpasswort festgelegt und aktiviert, dann muss der Benutzer nach jedem Neustart des Protector bei Zugriff auf eine beliebige HTTP URL dieses Passwort angeben, damit VPN-Verbindungen möglich sind. Wollen Sie diese Option nutzen, legen Sie im entsprechenden Eingabefeld das Nutzerpasswort fest.

Rootpasswort

Werksseitig voreingestellt: **root**
Wollen Sie das Rootpasswort ändern, geben Sie ins Feld *Altes Passwort* das alte Passwort ein, in die beiden Felder darunter das neue gewünschte Passwort.

Administratorpasswort (Account: admin)

Werksseitig voreingestellt: Protector (unveränderbarer Benutzername: admin)

Aktiviere Nutzerpasswort: Nein / Ja

Werksseitig ist Nutzer-Passwortschutz ausgeschaltet.
Ist unten ein Nutzerpasswort festgelegt, kann der Nutzer-Passwortschutz mit diesem Schalter aktiviert bzw. deaktiviert werden.

Nutzerpasswort

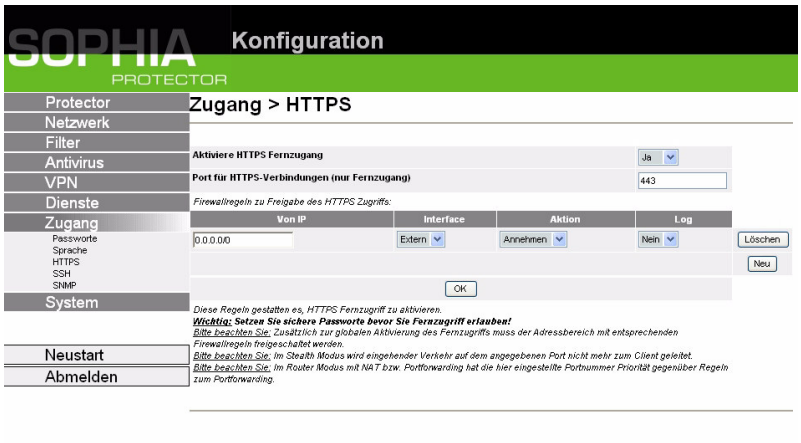
Werksseitig ist kein Nutzerpasswort voreingestellt. Um eines festzulegen, geben Sie in beide Eingabefelder übereinstimmend das gewünschte Passwort ein.

Zugang → Sprache

Bitte wählen Sie eine Sprache aus

Ist in der Sprachauswahlliste **(Automatisch)** ausgewählt, übernimmt das Gerät die Spracheinstellung aus dem Browser des Rechners.

Zugang → HTTPS



Bei eingeschaltetem HTTPS Fernzugang kann der Protector über seine webbasierte Administratoroberfläche von einem entfernten Rechner aus konfiguriert werden. Das heißt, auf dem entfernten Rechner wird der Browser benutzt, um den lokalen Protector zu konfigurieren.
Standardmäßig ist diese Option ausgeschaltet.

WICHTIG: Wenn Sie Fernzugriff ermöglichen, achten Sie darauf, dass ein sicheres Root- und Administrator-Passwort festgelegt ist.

Um HTTPS Fernzugang zu ermöglichen, machen Sie nachfolgende Einstellungen:

Aktiviere HTTPS Fernzugang: Ja / Nein

Wollen Sie HTTPS Fernzugriff ermöglichen, setzen Sie diesen Schalter auf **Ja**.

⌦ Achten Sie in diesem Fall darauf, die auf dieser Seite befindlichen Firewall-Regeln so zu setzen, dass von außen auf den Protector zugegriffen werden kann.

Port für HTTPS-Verbindungen (nur Fernzugang)

Standard: 443

Sie können einen anderen Port festlegen.

Die entfernte Gegenstelle, die den Fernzugriff ausübt, muss bei der Adressenangabe hinter die IP-Adresse die Port-Nummer angeben, die hier festgelegt ist.

Beispiel:

Ist dieser Protector über die Adresse 192.144.112.5 über das Internet zu erreichen, und ist für den Fernzugang die Port-Nummer 443 festgelegt, dann muss bei der entfernten Gegenstelle im Web-Browser diese Port-Nummer nicht hinter der Adresse angegeben werden.

Bei einer anderen Port-Nummer ist diese hinter der IP-Adresse anzugeben, z. B. wie folgt: 192.144.112.5:442

Firewall-Regeln zu Freigabe des HTTPS-Zugriffs

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenpakete eines HTTP-Fernzugriffs.

Regel löschen

☞ Klicken Sie neben dem betreffenden Eintrag **Löschen**.

Neue Regel setzen

☞ Wollen Sie eine neue Regel zu setzen, klicken Sie **Neu**.

Legen Sie die gewünschte Regel fest (s. u.) und klicken Sie **OK**.

Von IP

Geben Sie hier die Adresse(n) des/der Rechners an, dem/denen Fernzugang erlaubt ist.

Bei den Angaben haben Sie folgende Möglichkeiten:

- IP-Adresse: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)” auf Seite 77

Interface

extern (fest vorgegeben).

Aktion

Möglichkeiten: *Annehmen / Abweisen / Verwerfen*

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat *Abweisen* dieselbe Wirkung wie *Verwerfen* - s. u.)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

⌦ Im Stealth-Modus ist *Abweisen* als Aktion nicht möglich.

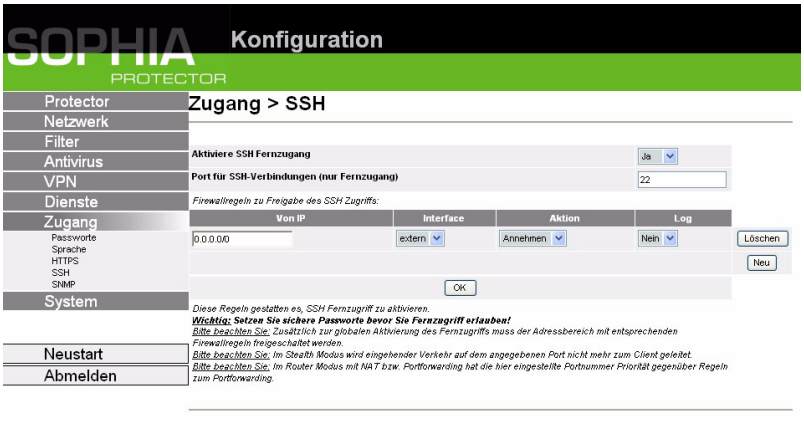
Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

☞ das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen

☞ oder nicht - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

Zugang → SSH



Bei eingeschaltetem SSH Fernzugang kann der Protector von einem entfernten Rechner aus konfiguriert werden - durch Kommandozeilen-Eingabe.
Standardmäßig ist diese Option ausgeschaltet.

WICHTIG: Wenn Sie Fernzugriff ermöglichen, achten Sie darauf, dass ein sicheres Root- und Administrator-Passwort festgelegt ist.

Um SSH Fernzugang zu ermöglichen, machen Sie folgende Einstellungen:

Aktiviere SSH Fernzugang: Ja / Nein

Wollen Sie SSH Fernzugriff ermöglichen, setzen Sie diesen Schalter auf **Ja**.

⌦ Achten Sie in diesem Fall darauf, die auf dieser Seite befindlichen Firewall-Regeln so zu setzen, dass von außen auf den Protector zugegriffen werden kann.

Port für SSH-Verbindungen (nur Fernzugang)

Standard: 22
Sie können einen anderen Port festlegen.

Die entfernte Gegenstelle, die den Fernzugriff ausübt, muss bei der Adressenangabe hinter die IP-Adresse die Port-Nummer angeben, die hier festgelegt ist.
Beispiel:

Ist dieser Protector über die Adresse 192.144.112.5 über das Internet zu erreichen, und ist für den Fernzugang die Port-Nummer 22 festgelegt, dann muss bei der entfernten Gegenstelle im SSH-Client (z. B. Web-Browser) diese Port-Nummer nicht angegeben werden.
Bei einer anderen Port-Nummer (z. B. 22222) ist diese anzugeben, z. B.:
ssh -p 22222 192.144.112.5

Firewall-Regeln zu Freigabe des SSH-Zugriffs

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenpakete eines SSH-Fernzugriffs.

Regel löschen

☞ Klicken Sie neben dem betreffenden Eintrag **Löschen**.

Neue Regel setzen

☞ Wollen Sie eine neue Regel zu setzen, klicken Sie **Neu**.
Legen Sie die gewünschte Regel fest (s. u.) und klicken Sie **OK**.

Von IP

Geben Sie hier die Adresse(n) des/der Rechners an, dem/denen Fernzugang erlaubt ist.
Bei den Angaben haben Sie folgende Möglichkeiten:

- IP-Adresse: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)" auf Seite 77

Interface

extern (fest vorgegeben).

Aktion

Möglichkeiten: *Annehmen / Abweisen / Verwerfen*

Annehmen bedeutet, die Datenpakete dürfen passieren.
Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat *Abweisen* dieselbe Wirkung wie *Verwerfen*.)
Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

⌦ Im Stealth-Modus ist *Abweisen* als Aktion nicht möglich.

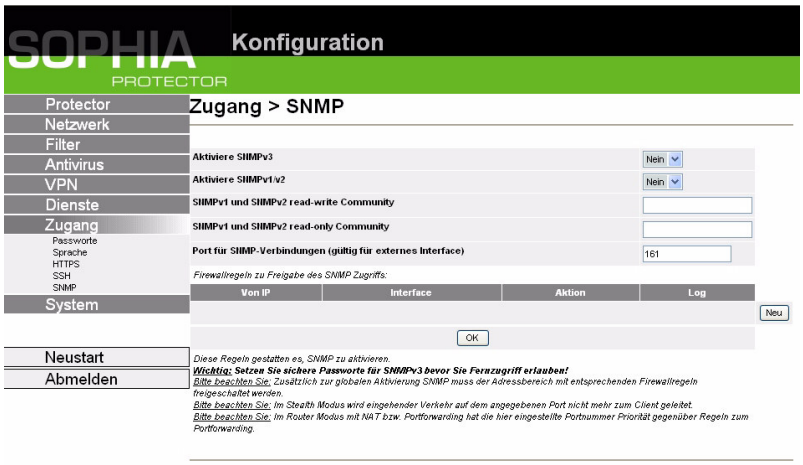
Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

☞ das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen

☞ oder nicht - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

Zugang → SNMP (nur Protector M,L)



Das SNMP (Simple Network Management Protokoll) wird vorzugsweise in komplexeren Netzwerken benutzt, um den Zustand und den Betrieb von Geräten zu überwachen.
Das SNMP gibt es in mehreren Entwicklungsstufen: SNMPv1/SNMPv2 und SNMPv3.

Die älteren Versionen SNMPv1/SNMPv2 benutzen keine Verschlüsselung und gelten als nicht sicher. Daher ist davon abzuraten, SNMPv1/SNMPv2 zu benutzen.

SNMPv3 ist unter dem Sicherheitsaspekt deutlich besser, wird aber noch nicht von allen Management-Konsolen unterstützt.

⌦ SNMP-„Get"- oder „Walk"-Anfragen können länger als eine Sekunde dauern. Dieser Wert entspricht jedoch dem Standard-Timeout-Wert einiger SNMP-Management-Applikationen.

Bitte setzen Sie aus diesem Grund den Timeout-Wert Ihrer Management Applikation auf Werte zwischen 3 und 5 Sekunden, falls Timeout-Probleme auftreten sollten.

Aktiviere SNMPv3: Ja / Nein

Wollen Sie zulassen, dass der Protector per SNMPv3 überwacht werden kann, setzen Sie diesen Schalter auf **Ja**.

Für den Zugang per SNMPv3 ist eine Authentifizierung mittels Login und Paßwort notwendig. Die Werkseinstellungen für die Login-Parameter lauten:

Login: admin

Passwort: SnmpAdmin

Für die Authentifizierung wird MD5 unterstützt, für die Verschlüsselung DES.

Die Login-Parameter für SNMPv3 können nur mittels SNMPv3 geändert werden.

Aktiviere SNMPv1/v2: Ja / Nein

Wollen Sie zulassen, dass der Protector per SNMPv1/v2 überwacht werden kann, setzen Sie diesen Schalter auf **Ja**.

Zusätzlich müssen Sie die nachfolgenden Login-Daten angeben:

SNMPv1 und SNMPv2 read-write Community

SNMPv1 und SNMPv2 read-only Community

Geben Sie in diese Felder die erforderlichen Login-Daten ein.

Port für SNMP-Verbindungen (gültig für externes Interface)

Standard: 161

Mit externem Interface ist die Schnittstelle des Protector nach außen gemeint, also z. B. zum Internet.

Firewall-Regeln zu Freigabe des SNMP-Zugriffs

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenpakete eines SNMP-Zugriffs.

Regel löschen

☞ Klicken Sie neben dem betreffenden Eintrag **Löschen**.

Neue Regel setzen

☞ Wollen Sie eine neue Regel zu setzen, klicken Sie **Neu**.

Legen Sie die gewünschte Regel fest (s. u.) und klicken Sie **OK**.

Von IP

Geben Sie hier die Adresse(n) des/der Rechners an, dem/denen SNMP-Überwachung erlaubt ist.

Bei den Angaben haben Sie folgende Möglichkeiten:

- Von IP

  0.0.0.0/0 bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)" auf Seite 77.

Interface

extern (fest vorgegeben).

Aktion

Möglichkeiten: *Annehmen / Abweisen / Verwerfen*
Annehmen bedeutet, die Datenpakete dürfen passieren.
Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat *Abweisen* dieselbe Wirkung wie *Verwerfen*.)
Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.
⌦ Im Stealth-Modus ist *Abweisen* als Aktion nicht möglich.

Log

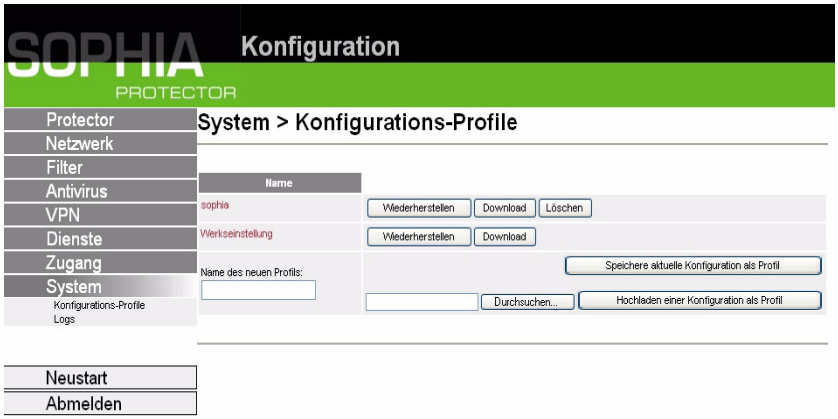
Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

☞ das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen

☞ oder nicht - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

5.11 Menü System

System → Konfigurations-profile



Sie haben die Möglichkeit, die Einstellungen des Protector als Konfigurations-Profil unter einem beliebigen Namen im Protector zu speichern. Sie können mehrere solcher Konfigurations-Profile anlegen. Dann können Sie bei Bedarf mal das eine, mal das andere Konfigurations-Profil aktivieren, wenn Sie den Protector in unterschiedlichen Betriebsumgebungen einsetzen.
Darüber hinaus können Sie Konfigurations-Profile als Dateien auf der Festplatte des Konfigurations-Rechners abspeichern. Umgekehrt besteht die Möglichkeit, eine so erzeugte Konfigurationsdatei in den Protector zu laden und in Kraft zu setzen.
Zusätzlich haben Sie die Möglichkeit, jederzeit die Werkseinstellung (wieder) in Kraft zu setzen.

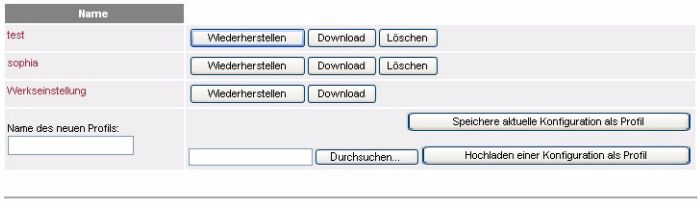
⌦ Beim Abspeichern eines Konfigurations-Profils werden Passwörter und Benutzernamen nicht mitgespeichert.

Aktuelle Konfiguration als Konfigurations-Profil im Protector speichern

1. In Feld *Name des neuen Profils* den gewünschten Namen eintragen
2. Die Schaltfläche **Speichere aktuelle Konfiguration als Profil** klicken.

Ein im Protector gespeichertes Konfigurations-Profil anzeigen /aktivieren / löschen

Namen angelegter Konfigurations-Profile (Beispiel)



Voraussetzung: Es ist mindestens ein Konfigurations-Profil angelegt und im Protector gespeichert (s. o.).

Konfigurations-Profil anzeigen:
Den Namen des Konfigurations-Profils anklicken.

Konfigurations-Profil aktivieren:
Rechts neben dem Namen des betreffenden Konfigurations-Profils die Schaltfläche **Wiederherstellen** klicken.

Konfigurations-Profil löschen:
Rechts neben dem Namen des betreffenden Konfigurations-Profils die Schaltfläche **Löschen** klicken.

Werkseinstellung anzeigen / aktivieren

Die Werkseinstellung ist als Konfigurations-Profil unter dem Namen *Factory Default* im Protector gespeichert.

Anzeigen: Den Namen *Factory Default* anklicken.

Aktivieren: Neben dem Namen *Factory Default* die Schaltfläche **Wiederherstellen** klicken.

⌦ Es ist nicht möglich, das Konfigurations-Profil *Factory Default* zu löschen.

Konfigurations-Profil als Datei auf Festplatte speichern

1. Rechts neben dem Namen des betreffenden Konfigurations-Profils die Schaltfläche **Download** klicken.
2. Legen Sie im angezeigten Dialogfeld den Dateinamen und Ordner fest, unter bzw. in dem das Konfigurations-Profil als Datei gespeichert wird.
   (Sie können die Datei beliebig benennen.)

Konfigurations-Profil von Festplatte in Protector laden

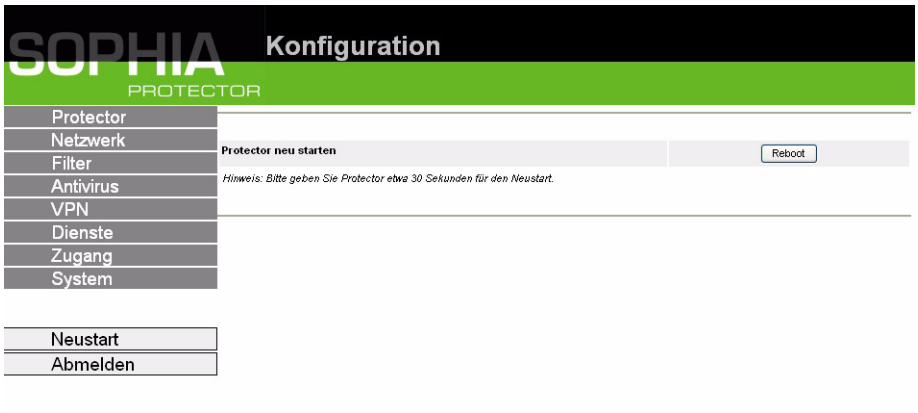
Voraussetzung: Sie haben nach dem oben beschriebenem Verfahren ein Konfigurations-Profil als Datei auf der Festplatte des Konfigurations-Rechners gespeichert.

1. In Feld *Name des neuen Profils* den Namen eintragen, den das einzuladende Konfigurations-Profil erhalten soll.
2. Die Schaltfläche **Durchsuchen** klicken und dann die Datei selektieren.
3. Die Schaltfläche **Hochladen einer Konfiguration als Profil** klicken.
   Folge: Die hochgeladene Konfiguration erscheint in der Liste der Konfigurations-Profile.

Soll das hochgeladene Konfigurations-Profil aktiviert werden, klicken Sie neben dem Namen auf **Wiederherstellen.**

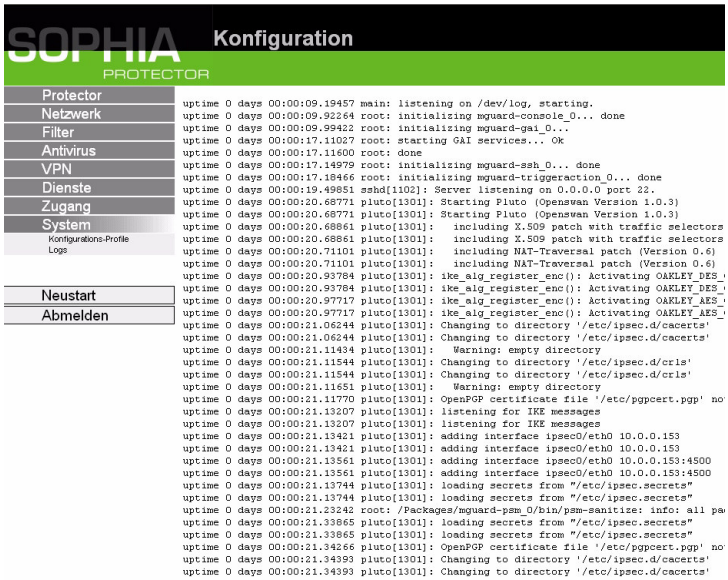
⌦ Wenn das Wiederherstellen einen Wechsel zwischen dem Stealth-Modus und einem der anderen Netzwerk-Modi beinhaltet, wird der Protector neu gestartet.

System → Neustart



Ein Neustart (= Reboot) ist erforderlich im Fehlerfall. Außerdem kann es erforderlich sein nach einem Software-Update.
Am Ende des Neustarts erscheint der Text „Neu gestartet“.
Ein Reboot kann auch durch aus- und wieder einschalten bewirkt werden.

System → Logs



Nur Anzeige

Zeigt alle aufgezeichneten Log-Einträge (Gesamtlog).
Das Format entspricht dem unter Linux gebräuchlichen Format.
Es gibt spezielle Auswertungsprogramme, die Ihnen die Informationen aus den protokollierten Daten in einem besser lesbaren Format präsentieren.
Sie können die Log-Einträge auf einen externen Server übertragen. Siehe „Dienste → Remote Logging (nur Protector M,L)” auf Seite 67.

5.12 CIDR (Classless InterDomain Routing)

IP Netzmasken und CIDR sind Notationen, die mehrere IP-Adressen zu einem Adressraum zusammenfassen. Dabei wird ein Bereich von aufeinanander folgenden Adressen als ein Netzwerk behandelt.

Das CIDR-Verfahren reduziert die z. B. in Routern gespeicherten Routing-Tabellen durch ein Postfix in der IP-Adresse. Mit diesem Postfix kann ein Netz und die darunter liegende Netze zusammengefasst bezeichnet werden. Die Methode ist in RFC 1518 beschrieben.

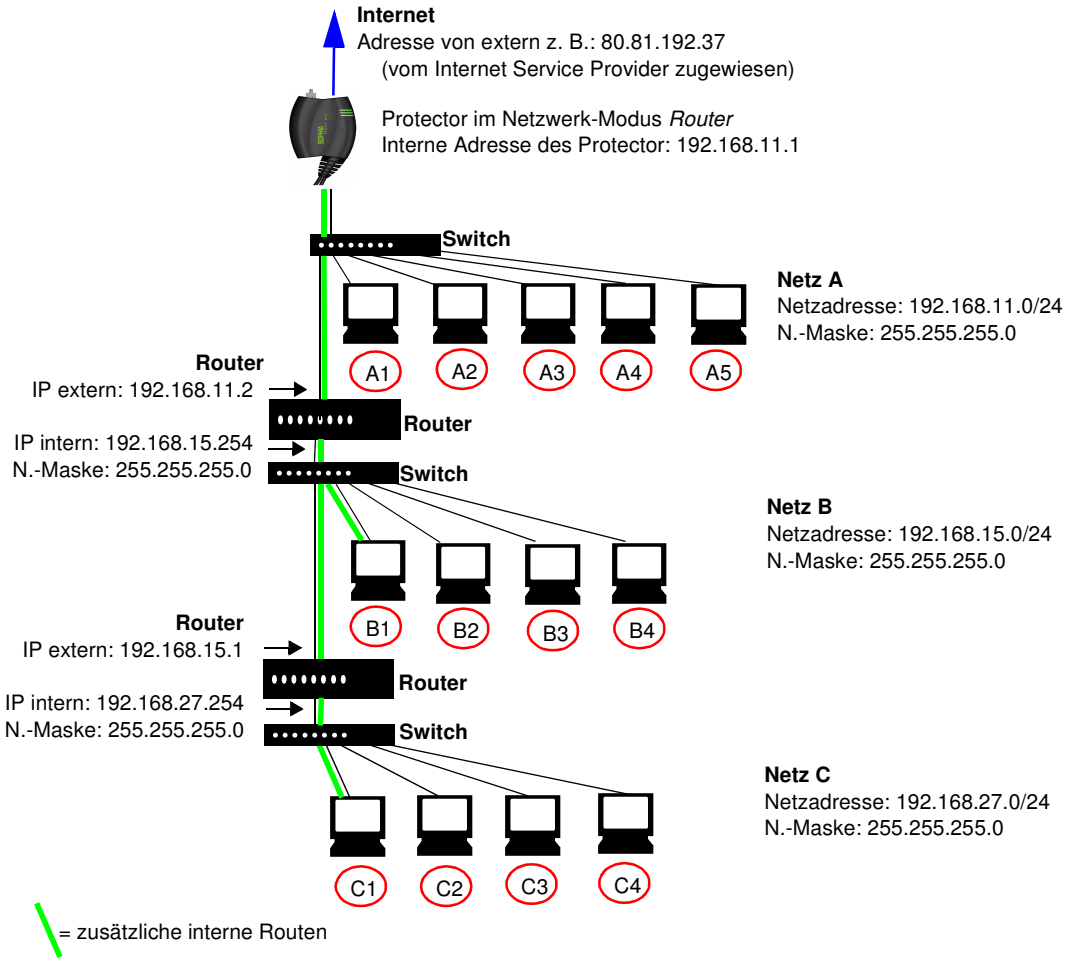
Um dem Protector einen Bereich von IP-Adressen anzugeben z. B. bei der Konfiguration der Firewall, kann es erforderlich sein, den Adressraum in der CIDR-Schreibweise anzugeben. Die nachfolgende Tabelle zeigt links die IP-Netzmaske, ganz rechts die entsprechende CIDR-Schreibweise.

IP-Netzmaske	binär				CIDR
255.255.255.255	11111111	11111111	11111111	11111111	32
255.255.255.254	11111111	11111111	11111111	11111110	31
255.255.255.252	11111111	11111111	11111111	11111100	30
255.255.255.248	11111111	11111111	11111111	11111000	29
255.255.255.240	11111111	11111111	11111111	11110000	28
255.255.255.224	11111111	11111111	11111111	11100000	27
255.255.255.192	11111111	11111111	11111111	11000000	26
255.255.255.128	11111111	11111111	11111111	10000000	25
255.255.255.0	11111111	11111111	11111111	00000000	24
255.255.254.0	11111111	11111111	11111110	00000000	23
255.255.252.0	11111111	11111111	11111100	00000000	22
255.255.248.0	11111111	11111111	11111000	00000000	21
255.255.240.0	11111111	11111111	11110000	00000000	20
255.255.224.0	11111111	11111111	11100000	00000000	19
255.255.192.0	11111111	11111111	11000000	00000000	18
255.255.128.0	11111111	11111111	10000000	00000000	17
255.255.0.0	11111111	11111111	00000000	00000000	16
255.254.0.0	11111111	11111110	00000000	00000000	15
255.252.0.0	11111111	11111100	00000000	00000000	14
255.248.0.0	11111111	11111000	00000000	00000000	13
255.240.0.0	11111111	11110000	00000000	00000000	12
255.224.0.0	11111111	11100000	00000000	00000000	11
255.192.0.0	11111111	11000000	00000000	00000000	10
255.128.0.0	11111111	10000000	00000000	00000000	9
255.0.0.0	11111111	00000000	00000000	00000000	8
254.0.0.0	11111110	00000000	00000000	00000000	7
252.0.0.0	11111100	00000000	00000000	00000000	6
248.0.0.0	11111000	00000000	00000000	00000000	5
240.0.0.0	11110000	00000000	00000000	00000000	4
224.0.0.0	11100000	00000000	00000000	00000000	3
192.0.0.0	11000000	00000000	00000000	00000000	2
128.0.0.0	10000000	00000000	00000000	00000000	1
0.0.0.0	00000000	00000000	00000000	00000000	0

Beispiel: 192.168.1.0 / 255.255.255.0 entspricht im CIDR: 192.168.1.0/24

5.13 Netzwerk-Beispielskizze

Die nachfolgende Skizze zeigt, wie in einem lokalen Netzwerk mit Subnetzen die IP-Adressen veteilt sein könnten, welche Netzwerk-Adressen daraus resultieren und wie die Angabe einer zusätzlichen internen Route lauten könnte.



Netz A

Rechner	A1	A2	A3	A4	A5
IP-Adresse	192.168.11.3	192.168.11.4	192.168.11.5	192.168.11.6	192.168.11.7
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Netz B

Rechner	B1	B2	B3	B4
IP-Adresse	192.168.15.2	192.168.15.3	192.168.15.4	192.168.15.5
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Netz C

Rechner	C1	C2	C3	C4
IP-Adresse	192.168.27.1	192.168.27.2	192.168.27.3	192.168.27.4
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Zusätzliche interne Routen:
Netzwerk: 192.168.15.0/24
Gateway: 192.168.11.2

Netzwerk: 192.168.27.0/24
Gateway: 192.168.11.2

6 Die Recovery-Taste für Neustart, Recovery-Prozedur und Flashen der Firmware

Die Recovery-Taste wird benutzt, um das Gerät in einen der folgenden Zustände zu bringen:

Neustart durchführen

Ziel Das Gerät neu starten mit den konfigurierten Einstellungen.

Aktion: **Recovery**-Taste für ca. 1,5 Sekunden drücken, z. B. mit einer aufgebogenen Büroklammer, bis die mittlere LED rot leuchtet.
ODER
Die Stromzufuhr vorübergehend unterbrechen.

.

6.1 Recovery-Prozedur ausführen

Ziel Der Protector soll in den Netzwerk-Modus (= Betriebsart) **Stealth** zurückgeschaltet werden, so dass er für Konfigurationszwecke wieder erreichbar ist unter folgender Adresse: **https://1.1.1.1/**

⌦ Die konfigurierten Einstellungen für VPN-Verbindungen und Firewall bleiben erhalten, ebenso Passwörter.

Mögliche Gründe zum Ausführen der Recovery-Prozedur:
Der Protector befindet sich im Router- oder PPPoE-Modus und
– die Geräteadresse des Protector ist konfiguriert worden abweichend von der Standardeinstellung und
– Sie kennen die aktuelle IP-Adresse des Gerätes nicht.

Aktion:

1. Führen Sie einen Neustart durch - siehe oben.
2. Warten Sie, bis die Heartbeat-LED blinkt (mittlere LED grün blinkend). Dauert ca. 30 Sekunden.
3. Die **Recovery**-Taste langsam 6-mal drücken.
   Folge:
   Nach ca. 2 Sekunden antwortet der Protector:
   Die mittlere LED blinkt 6-mal in Rot.
4. Innerhalb der nächsten 60 Sekunden erneut die **Recovery**-Taste 6 mal drücken.
   Folge:
   Das Gerät vollzieht einen Neustart und schaltet sich dabei auf den *Stealth*-Modus. Es ist dann wieder unter folgender Adresse zu erreichen:
   https://1.1.1.1/

6.2 Flashen der Firmware

Ziel Die gesamte Software des Protector soll neu ins Gerät geladen werden.

⌦ **Alle konfigurierten Einstellungen werden gelöscht.** Der Protector wird in den Auslieferungszustand versetzt.

Mögliche Gründe zum Flashen der Firmware:
- Das Administrator-Passwort ist verloren gegangen.
- Die Firewall-Regeln wurden so eingestellt, dass der Administrator-Zugang nicht mehr erfolgen kann.

Aktion: Gehen Sie wie folgt vor:

⌦ **Sie dürfen während der gesamten Flash-Prozedur auf keinen Fall die Stromversorgung des Protector unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.**

Voraussetzungen:
- Sie haben die Software des Protector von der Protector-CD kopiert oder vom SOPHIA-Support bezogen und auf dem Konfigurations-Rechner gespeichert.
- DHCP- und TFTP-Server sind auf demselben Rechner installiert - siehe „Voraussetzungen zum Flashen der Firmware: DHCP- und TFTP-Server" auf Seite 81.

1. **Recovery**-Taste gedrückt halten, bis der *Recovery-Status* wie folgt eintritt:

   Der Protector wird neu gestartet (nach a. 1,5 Sekunden), nach weiteren ca. 1,5 Sekunden gelangt der Protector in den *Recovery-Status*.
   Statusanzeige des *Recovery-Status*: Alle LEDs leuchten in Grün.

2. Spätestens 1 Sekunde nach Eintritt des *Recovery-Status* die **Recovery**-Taste loslassen.
   (Falls Sie die **Recovery**-Taste nicht loslassen, wird der Protector neu gestartet.)
   Folge:
   Der Protector startet das Recovery-System. Er sucht über die Schnittstelle für den lokal angeschlossenen Rechner bzw. das lokal angeschlossene Netzwerks nach dem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.
   - Statusanzeige: Die mittlere LED (Heartbeat) blinkt.
     Vom TFTP-Server wird die Datei install.p7s geladen. Diese enthält die elektronisch unterschriebene Kontrollprozedur für den Installationsvorgang. Nur von Innominate unterschriebene Dateien werden geladen.
     Die Kontrollprozedur löscht nun den Flashspeicher und bereitet die Neuinstallation der Software vor.

- Statusanzeige: Die 3 grünen LEDs bilden ein Lauflicht.
  Dann wird vom TFTP-Server die Software jffs2.img.p7s heruntergeladen und in den Flashspeicher geschrieben. Diese Datei enthält das eigentliche Protector-Betriebssystem und ist elektronisch signiert. Nur von Innominate signierte Dateien werden akzeptiert.
- Statusanzeige: Die 3 grünen LEDs bilden ein Lauflicht.
  Das Löschen und Schreiben dauert ca. 3 bis 5 Minuten.
  Dann wird der Protector automatisch neu gestartet.
  Die neue Software wird entpackt und konfiguriert. Das dauert ca. 5 Minuten.
- Statusanzeige: Die mittlere LED (Heartbeart) leuchtet kontinuierlich.
  Sobald die Prozedur beendet ist, blinken alle 3 LEDs gleichzeitig in Grün.

3. Starten Sie den Protector neu.
   Drücken Sie dazu kurz die **Recovery**-Taste.
   ODER
   Unterbrechen Sie seine Stromversorgung und schließen Sie ihn dann wieder an (per USB-Kabel, das ausschließlich zur Stromversorgung dient).

   Folge:
   Der Protector befindet sich im Auslieferungs-Zustand. Konfigurieren Sie ihn neu - siehe „Lokale Konfigurationsverbindung herstellen” auf Seite 13.

Voraussetzungen zum Flashen der Firmware: DHCP- und TFTP-Server

Zum "Flashen" der Firmware muss auf dem lokal angeschlossenen Rechner bzw. Netzwerk-Rechner ein DHCP- und TFTP-Server installiert sein.
(DHCP = **D**ynamic **H**ost **C**onfiguration **P**rotocol; TFTP = **T**rivial **F**ile **T**ransfer **P**rotocol)

Installieren Sie den DHCP- und TFTP-Server, falls notwendig (siehe unten).

⌦ Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden!

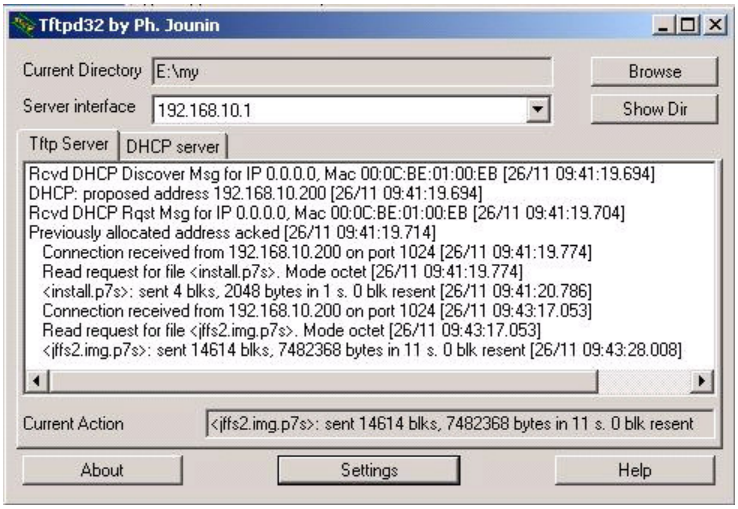
6.2.1 DHCP- und TFTP-Server unter Windows bzw. Linux installieren

Unter Windows:

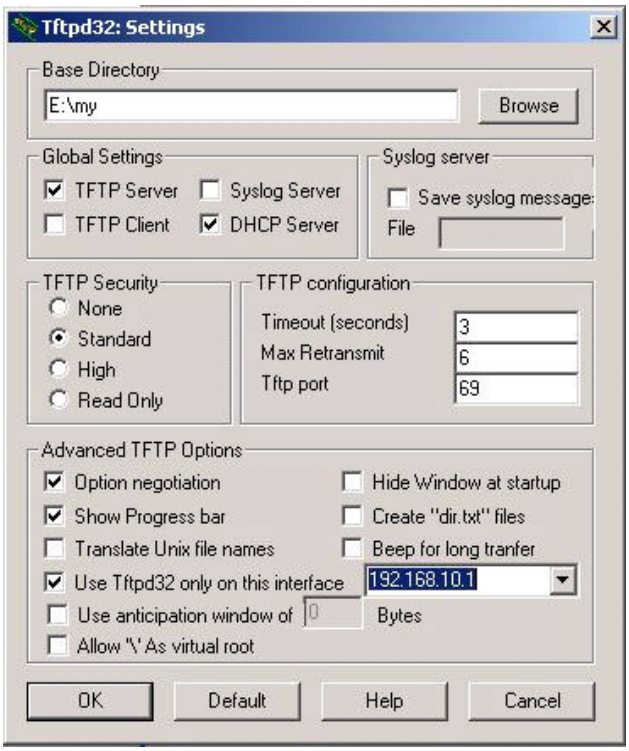
Installieren Sie das Programm, das sich auf der CD befindet. Gehen Sie dazu wie folgt vor:

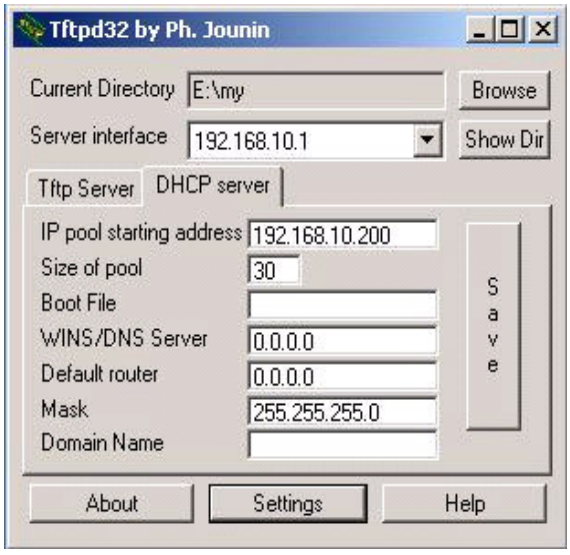
1. Ist der Windows-Rechner an einem Netzwerk angeschlossen, trennen Sie ihn von diesem.
2. Kopieren Sie die Software in einen beliebigen leeren Ordner des Windows-Rechners. Starten Sie das Programm TFTPD32.EXE
3. Die festzulegende Host-IP lautet: **192.168.10.1.** Das muss auch die Adresse für die Netzwerkkarte sein.
   Klicken Sie die Schaltfläche **Browse**, um auf den Ordner zu wechseln, wo die Protector-Imagedateien gespeichert sind: *install.p7s, jffs2.img.p7s*

Die Image-Dateien befinden sich auch auf der CD, die zum Lieferumfang gehört.



4. Wechseln Sie auf die Registerkarte Tftp Server bzw. DHCP Server und klikken Sie dann die Schaltfläche Settings, um im dann angezeigten Dialogfeld die Parameter wie folgt zu setzen:





Unter Linux

Alle aktuellen Linux-Distributionen enthalten DHCP- und TFTP-Server. Installieren Sie die entsprechenden Pakete gemäß der Anleitung der jeweiligen Distribution.
Konfigurieren Sie den DHCP-Server, indem Sie in der Datei **/etc/dhcp** folgende Einstellungen vornehmen:

```
subnet 192.168.134.0 netmask 255.255.255.0 {
range 192.168.134.100 192.168.134.119;
option routers 192.168.134.1;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.134.255;}
```

Diese Beispiel-Konfiguration stellt 20 IP-Adressen (.100 bis .119) bereit. Es wird angenommen, dass der DHCP-Server die Adresse 192.168.134.1 hat (Einstellungen für ISC DHCP 2.0).

Der benötigte TFTP-Server wird in folgender Datei konfiguriert:
/etc/inetd.conf
Fügen Sie in diese Datei die entsprechende Zeile ein oder setzen Sie die notwendigen Parameter für den TFTP-Service. (Verzeichnis für Daten ist: **/tftpboot)**

```
tftp dgram udp wait root /usr/sbin/in.tftpd -s /tftpboot/
```

Starten Sie dann den inetd-Prozess neu, um die Konfigurationsänderungen zu übernehmen.
Sollten Sie einen anderen Mechanismus verwenden, z. B. xinetd, dann informieren Sie sich bitte in der entsprechenden Dokumentation.

7 Glossar

Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung werden Daten mit einem Schlüssel verschlüsselt und mit einem zweiten Schlüssel wieder entschlüsselt. Beide Schlüssel eignen sich zum Ver- und Entschlüsseln. Einer der Schlüssel wird von seinem Eigentümer geheim gehalten (Privater Schlüssel/Private Key), der andere wird der Öffentlichkeit (Öffentlicher Schlüssel/Public Key), d. h. möglichen Kommunikationspartnern, gegeben.
Eine mit dem öffentlichen Schlüssel verschlüsselte Nachricht kann nur von dem Empfänger entschlüsselt und gelesen werden, der den zugehörigen privaten Schlüssel hat. Eine mit dem privaten Schlüssel verschlüsselte Nachricht kann von jedem Empfänger entschlüsselt werden, der den zugehörigen öffentlichen Schlüssel hat. Die Verschlüsselung mit dem privaten Schlüssel zeigt, daß die Nachricht tatsächlich vom Eigentümer des zugehörigen öffentlichen Schlüssels stammt. Daher spricht man auch von digitaler Signatur, Unterschrift.
Assymetrische Verschlüsselungsverfahren wie RSA sind jedoch langsam und anfällig für bestimmte Angriffe, weshalb sie oft mit einem symmetrischen Verfahren kombiniert werden (→ symmetrische Verschlüsselung). Andererseits sind Konzepte möglich, die die aufwendige Administrierbarkeit von symmetrischen Schlüsseln vermeiden.

DES / 3DES

Der von IBM stammende und von der NSA überprüfte symmetrische Verschlüsselungsalgorithmus (→ symmetrische Verschlüsselung) DES wurde 1977 vom amerikanischen National Bureau of Standards, dem Vorgänger des heutigen National Institute of Standards and Technology (NIST), als Standard für amerikanische Regierungsinstitutionen festgelegt. Das es sich hierbei um den ersten standardisierten Verschlüsslungsalgorithmus überhaupt handelte, setzte er sich auch schnell in der Industrie und somit außerhalb Amerikas durch.
DES arbeitet mit einer Schlüssellänge von 56Bit, die heute aufgrund der seit 1977 gestiegenen Rechenleistung der Computer als nicht mehr sicher gilt.
3DES ist eine Variante von DES. Es arbeitet mit 3 mal größeren Schlüsseln, die also 168 Bit lang sind. Sie gilt heute noch als sicher und ist unter anderem auch Teil des IPsec-Standards.

AES

Das NIST (National Institute of Standards and Technology) entwickelt in Zusammenarbeit mit Industrie-Unternehmen seit Jahren den AES-Verschlüsselungsstandard. Diese → symmetrische Verschlüsselung soll den bisherigen DES-Standard ablösen. Der AES-Standard spezifiziert drei verschiedene Schlüsselgrößen mit 128, 192 und 256 Bit.
1997 hatte die NIST die Initiative zu AES gestartet und ihre Bedingungen für den Algorithmus bekannt gegeben. Von den vorgeschlagenen Verschlüsselungsalgorithmen hat die NIST fünf Algorithmen in die engere Wahl gezogen; und zwar die Algorithmen MARS, RC6, Rijndael, Serpent und Twofish. Im Oktober 2000 hat man sich für Rijndael als Verschlüsselungsalgorithmus entschieden.

Client / Server

In einer Client-Server-Umgebung ist ein Server ein Programm oder Rechner, das vom Client-Programm oder Client-Rechner Anfragen entgegennimmt und beantwortet.
Bei Datenkommunikation bezeichnet man auch den Rechner als Client, der eine Verbindung zu einem Server (oder Host) herstellt. D. h. der Client ist der anrufende Rechner, der Server (oder Host) der angerufene.

Datagramm

Beim Übertragungsprotokoll TCP/IP werden Daten in Form von Datenpaketen, den sog. IP-Datagrammen, versendet. Ein IP-Datagramm hat folgenden Aufbau:

IP-Header	TCP, UDP, ESP etc. Header	Daten (Payload)

Der IP-Header enthält:
– die IP-Adresse des Absenders (source IP-address)
– die IP-Adresse des Empfängers (destination IP-adress)
– die Protokollnummer des Protokoll der nächst höheren Protokollschicht (nach dem OSI-Schichtenmodell)
– die IP-Header Prüfsumme (Checksum) zur Überprüfung der Integrität des Headers beim Empfang.

Der TCP-/UDP-Header enthält folgende Informationen:
– Port des Absenders (source port)
– Port des Empfängers (destination port)
– eine Prüfsume über den TCP-Header und ein paar Informationen aus dem IP-Header (u. a. Quell- und Ziel-IP-Adresse)

DynDNS-Anbieter

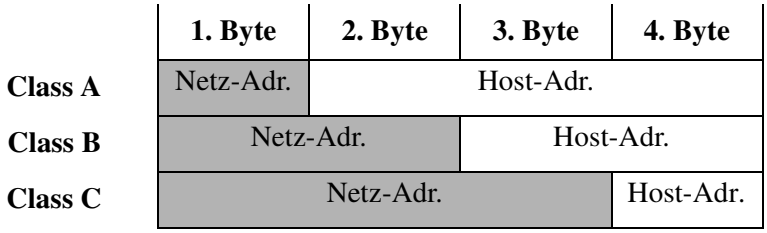
Auch *Dynamic DNS-Anbieter*. Jeder Rechner, der mit dem Internet verbunden ist, hat eine IP-Adresse (IP = Internet Protocol) Eine IP-Adresse besteht aus 4 maximal dreistelligen Nummern, jeweils durch einem Punkt getrennt. Ist der Rechner über die Telefonleitung per Modem, per ISDN oder auch per ADSL online, wird ihm vom Internet Service Provider dynamisch eine IP-Adresse zugeordnet, d. h. die Adresse wechselt von Sitzung zu Sitzung. Auch wenn der Rechner (z. B. bei einer Flatrate) über 24 Stunden ununterbrochen online ist, wird die IP-Adresse zwischendurch gewechselt.
Soll ein lokaler Rechner über das Internet erreichbar sein, muss er eine Adresse haben, die der entfernten Gegenstelle bekannt sein muss. Nur so kann diese die Verbindung zum lokalen Rechner aufbauen. Wenn die Adresse des lokalen Rechners aber ständig wechselt, ist das nicht möglich. Es sei denn, der Betreiber des lokalen Rechners hat ein Account bei einem DynamicDNS-Anbieter (DNS = Domain Name Server).
Dann kann er bei diesem einen Hostnamen festlegen, unter dem der Rechner künftig erreichbar sein soll, z. B.: www.xyz.abc.de. Zudem stellt der DynamicDNS-Anbieter ein kleines Programm zur Verfügung, das auf dem betreffenden Rechner installiert und ausgeführt werden muss. Bei jeder Internet-Sitzung des lokalen Rechners teilt dieses Tool dem DynamicDNS-Anbieter mit, welche IP-Adresse der Rechner zurzeit hat. Dessen Domain Name Server registriert die aktuelle Zuordnung Hostname - IP-Adresse und teilt diese anderen Domain Name Servern im Internet mit.
Wenn jetzt ein entfernte Rechner eine Verbindung herstellen will zum lokalen Rechner, der beim DynamicDNS-Anbieter registriert ist, benutzt der entfernte Rechner den Hostnamen des lokalen Rechners als Adresse. Dadurch wird eine Verbindung hergestellt zum zuständigen DNS (Domain Name Server), um dort die IP-Adresse nachzuschlagen, die diesem Hostnamen zurzeit zugeordnet ist. Die IP-Adresse wird zurückübertragen zum entfernten Rechner und jetzt von diesem als Zieladresse benutzt. Diese führt jetzt genau zum gewünschten lokalen Rechner.
Allen Internetadressen liegt im Grunde dieses Verfahren zu Grunde: Zunächst wird eine Verbindung zum DNS hergestellt, um die diesem Hostnamen zugeteilte IP-Adresse zu ermitteln. Ist das geschehen, wird mit dieser „nachgeschlagenen“ IP-Adresse die Verbindung zur gewünschten Gegenstelle, eine beliebige Internetpräsenz, aufgebaut.

IP-Adresse

Jeder Host oder Router im Internet / Intranet hat eine eindeutige IP-Adresse (IP = Internet Protocol). Die IP-Adresse ist 32 Bit (= 4 Byte) lang und wird geschrieben als 4 Zahlen (jeweils im Bereich 0 bis 255), die durch einen Punkt voneinander getrennt sind.
Eine IP-Adresse besteht aus 2 Teilen: die Netzwerk-Adresse und die Host-Adresse.

Netzwerk-Adresse	Host-Adresse

Alle Hosts eines Netzes haben dieselbe Netzwerk-Adresse, aber unterschiedliche Host-Adressen. Je nach Größe des jeweiligen Netzes - man unterscheidet Netze der Kategorie Class A, B und C - sind die beiden Adressanteile unterschiedlich groß:



Ob eine IP-Adresse ein Gerät in einem Netz der Kategorie Class A, B oder C bezeichnet, ist am ersten Byte der IP-Adresse erkennbar. Folgendes ist festgelegt:

	Wert des 1. Byte	**Bytes für die Netzadresse**	**Bytes für die Host-Adresse**
Class A	1 - 126	1	3
Class B	128 - 191	2	2
Class C	192 - 223	3	1

Rein rechnerisch kann es nur maximal 126 Class A Netze auf der Welt geben, jedes dieser Netze kann maximal 256 x 256 x 256 Hosts umfassen (3 Bytes Adressraum). Class B Netze können 64 x 256 mal vorkommen und können jeweils bis zu 65.536 Hosts enthalten (2 Bytes Adressraum: 256 x 256). Class C Netze können 32 x 256 x 256 mal vorkommen und können jeweils bis zu 256 Hosts enthalten (1 Byte Adressraum).

Subnetz-Maske

Einem Unternehmens-Netzwerk mit Zugang zum Internet wird normalerweise nur eine einzige IP-Adresse offiziell zugeteilt, z. B. 134.76.0.0. Bei dieser Beispiel-Adresse ist am 1. Byte erkennbar, dass es sich bei diesem Unternehmens-Netzwerk um ein Class B Netz handelt, d. h. die letzten 2 Byte können frei zur Host-Adressierung verwendet werden. Das ergibt rein rechnerisch einen Adressraum von 65.536 möglichen Hosts (256 x 256).
Ein so riesiges Netz macht wenig Sinn. Hier entsteht der Bedarf, Subnetze zu bilden. Dazu dient die Subnetz-Maske. Diese ist wie eine IP-Adresse ein 4 Byte langes Feld. Den Bytes, die die Netz-Adresse repräsentieren, ist jeweils der Wert 255 zugewiesen. Das dient vor allem dazu, sich aus dem Host-Adressenbereich einen Teil zu „borgen“, um diesen zur Adressierung von Subnetzen zu benutzen. So kann beim Class B Netz (2 Byte für Netzwerk-Adresse, 2 Byte für Host-Adresse) mit Hilfe der Subnetz-Maske 255.255.255.0 das 3. Byte, das eigentlich für Host-Adressierung vorgesehen war, jetzt für Subnetz-Adressierung verwen-

det werden. Rein rechnerisch können so 256 Subnetze mit jeweils 256 Hosts entstehen.

IPsec

IP Security (IPsec) ist ein Standard, der es ermöglicht, bei IP-Datagrammen (→ Datagramm) die Authentizität des Absenders, die Vertraulichkeit und die Integrität der Daten durch Verschlüsselung zu wahren. Die Bestandteile von IPsec sind der Authentication Header (AH), die Encapsulating-Security-Payload (ESP), die Security Association (SA) und der Internet Key Exchange (IKE).
Zu Beginn der Kommunikation klären die an der Kommunikation beteiligten Rechner das benutzte Verfahren und dessen Implikationen wie z. B. *Transport Mode* oder *Tunnel Mode*
Im *Transport Mode* wird in jedes IP-Datagramm zwischen IP-Header und TCP- bzw. UDP-Header ein IPsec-Header eingesetzt. Da dadurch der IP-Header unverändert bleibt, ist dieser Modus nur für eine Host- zu-Host-Verbindung geeignet.
Im *Tunnel Mode* wird dem gesamten IP-Datagramm ein IPsec-Header und ein neuer IP-Header vorangestellt. D. h. das ursprüngliche Datagramm wird insgesamt verschlüsselt in der Payload des neuen Datagramms untergebracht.
Der *Tunnel Mode* findet beim VPN Anwendung: Die Geräte an den Tunnelenden sorgen für die Ver- bzw. Entschlüsselung der Datagramme, auf der Tunnelstrekke, d. h. auf dem Übertragungsweg über ein öffentliches Netz bleiben die eigentlichen Datagramme vollständig geschützt.

NAT (Network Address Translation)

Bei der Network Address Translation (NAT) - oft auch als *IP-Masquerading* bezeichnet - wird hinter einem einzigen Gerät, dem sog. NAT-Router, ein ganzes Netzwerk „versteckt“. Die internen Rechner im lokalen Netz bleiben mit ihren IP-Adressen verborgen, wenn Sie nach außen über die NAT-Router kommunizieren. Für die Kommunikationspartner außen erscheint nur die NAT-Router mit ihrer eigenen IP-Adresse.
Damit interne Rechner dennoch direkt mit externen Rechnern (im Internet) kommunizieren können, muss die NAT-Router die IP-Datagramme verändern, die von internen Rechnern nach außen und von außen zu einem internen Rechner gehen.
Wird ein IP-Datagramm aus dem internen Netz nach außen versendet, verändert die NAT-Router den IP- und den TCP-Header des Datagramms. Sie tauscht die Quell-IP-Adresse und den Quell-Port aus gegen die eigene offizielle IP-Adresse und einen eigenen, bisher unbenutzen Port. Dazu führt sie eine Tabelle, die die Zuordnung der ursprünglichen mit den neuen Werten herstellt.
Beim Empfang eines Antwort-Datagramms erkennt die NAT-Router anhand des angegebenen Zielports, dass das Datagramm eigentlich für einen internen Rechner bestimmt ist. Mit Hilfe der Tabelle tauscht die NAT-Router die Ziel-IP-Adresse und den Ziel-Port aus und schickt das Datagramm weiter ins interne Netz.

Port-Nummer

Das Feld Port-Nummer ist ein 2 Byte großes Feld in UDP- und TCP-Headern. Die Vergabe der Port-Nummern dient der Identifikation der verschiedenen Datenströme, die UDP/TCP gleichzeitig abarbeitet. Über diese Port-Nummern erfolgt der gesamte Datenaustausch zwischen UDP/TCP und den Anwendungsprozessen. Die Vergabe der Port-Nummern an Anwendungsprozesse geschieht dynamisch und wahlfrei. Für bestimmte, häufig benutzte Anwendungsprozesse sind feste Port-Nummern vergeben. Diese werden als Assigned Numbers bezeichnet.

PPPoE

Akronym für **P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet. Basiert auf den Standards PPP und Ethernet. PPPoE ist eine Spezifikation, um Benutzer per Ethernet mit dem Internet zu verbinden über ein gemeinsam benutztes Breitbandmedium wie DSL, Wireless LAN oder Kabel-Modem.

PPTP

Akronym für **P**oint-to-**P**oint **T**unneling **P**rotocol. Entwickelt von Microsoft, U.S. Robotics und anderen wurde dieses Protokoll entwickelt, um zwischen zwei VPN-Knoten (→ VPN) über ein öffentliches Netz sicher Daten zu übertragen.

X.509 Zertifikat

Eine Art „Siegel“, welches die Echtheit eines öffentlichen Schlüssels (→ asymmetrische Verschlüsselung) und zugehöriger Daten belegt.

Damit der Benutzer eines zum Verschlüsseln dienenden öffentlichen Schlüssels sichergehen kann, dass der ihm übermittelte öffentliche Schlüssel wirklich von seinem tatsächlichen Aussteller und damit der Instanz stammt, die die zu versendenden Daten erhalten soll, gibt es die Möglichkeit der Zertifizierung. Diese Beglaubigung der Echtheit des öffentlichen Schlüssels und die damit verbundene Verknüpfung der Identität des Ausstellers mit seinem Schlüssel übernimmt eine zertifizierende Stelle (*Certification Authority - CA*). Dies geschieht nach den Regeln der CA, indem der Aussteller des öffentlichen Schlüssels beispielsweise persönlich zu erscheinen hat. Nach erfolgreicher Überprüfung signiert die CA den öffentliche Schlüssel mit ihrer (digitalen) Unterschrift, ihrer Signatur. Es entsteht ein Zertifikat.

Ein X.509(v3) Zertifikat beinhaltet also einen öffentlichen Schlüssel, Informationen über den Schlüsseleigentümer (angegeben als Distinguised Name (DN)), erlaubte Verwendungszwecke usw. und der Signatur der CA.

Die Signatur entsteht wie folgt: Aus der Bitfolge des öffentlichen Schlüssels, den Daten über seinen Inhaber und aus weiteren Daten erzeugt die CA eine individuelle Bitfolge, die bis zu 160 Bit lang sein kann, den sog. HASH-Wert. Diesen verschlüsselt die CA mit ihrem privaten Schlüssel und fügt ihn dem Zertifikat hinzu. Durch die Verschlüsselung mit dem privaten Schlüssel der CA ist die Echtheit belegt, d. h. die verschlüsselte HASH-Zeichenfolge ist die digitale Unterschrift der CA, ihre Signatur. Sollten die Daten des Zertifikats missbräuchlich geändert werden, stimmt dieser HASH-Wert nicht mehr, das Zertifikat ist dann wertlos.

Der HASH-Wert wird auch als Fingerabdruck bezeichnet. Da er mit dem privaten Schlüssel der CA verschlüsselt ist, kann jeder, der den zugehörigen öffentlichen Schlüssel besitzt, die Bitfolge entschlüsseln und damit die Echtheit dieses Fingerabdrucks bzw. dieser Unterschrift überprüfen.

Durch die Heranziehung von Beglaubigungsstellen ist es möglich, dass nicht jeder Schlüsseleigentümer den anderen kennen muss, sondern nur die benutzte Beglaubigungsstelle. Die zusätzlichen Informationen zu dem Schlüssel vereinfachen zudem die Administrierbarkeit des Schlüssels.

X.509 Zertifikate kommen z.B. bei Email Verschlüsselung mittels S/MIME oder IPsec zum Einsatz.

Protokoll, Übertragungsprotokoll

Geräte, die miteinander kommunizieren, müssen dieselben Regeln dazu verwenden. Sie müssen dieselbe „Sprache sprechen“. Solche Regeln und Standards bezeichnet man als Protokoll bzw. Übertragungsprotokoll. Oft benutze Protokolle sind z. B. IP, TCP, PPP, HTTP oder SMTP. TCP/IP ist der Oberbegriff für alle auf IP aufbauenden Protokolle.

Service Provider

Anbieter, Firma, Institution, die Nutzern den Zugang zum Internet oder zu einem Online-Dienst verschafft.

Spoofing, Antispoofing

In der Internet-Terminologie bedeutet Spoofing die Angabe einer falschen Adresse. Durch die falsche Internet-Adresse täuscht jemand vor, ein autorisierter Benutzer zu sein.
Unter Anti-Spoofing versteht man Mechanismen, die Spoofing entdecken oder verhindern.

Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung werden Daten mit dem gleichen Schlüssel ver- und entschlüsselt. Beispiele für symmetrische Verschlüsselungsalgorithmen sind DES und AES. Sie sind schnell, jedoch bei steigender Nutzerzahl nur aufwendig administrierbar.

TCP/IP (Transmission Control Protocol/ Internet Protocol)

Netzwerkprotokolle, die für die Verbindung zweier Rechner im Internet verwendet werden.
IP ist das Basisprotokoll.
UDP baut auf IP auf und verschickt einzelne Pakete. Diese können beim Empfänger in einer anderen Reihenfolge als der abgeschickten ankommen, oder sie können sogar verloren gehen.
TCP dient zur Sicherung der Verbindung und sorgt beispielsweise dafür, dass die Datenpakete in der richtigen Reihenfolge an die Anwendung weitergegeben werden.
UDP un TCP bringen zusätzlich zu den IP-Adressen Port-Nummern zwischen 1 und 65535 mit, über die die unterschiedlichen Dienste unterschieden werden.
Auf UDP und TCP bauen eine Reihe weiterer Protokolle auf, z. B. HTTP (Hyper Text Transfer Protokoll), HTTPS (Secure Hyper Text Transfer Protokoll), SMTP (Simple Mail Trnsfer Protokoll), POP3 (Post Office Protokoll, Version 3), DNS (Doamin Name Service).
ICMP baut auf IP auf und enthält Kontrollnachrichten.
SMTP ist ein auf TCP basierendes E-Mail-Protokoll.
IKE ist ein auf UDP basierendes IPsec-Protokoll.
ESP ist ein auf IP basierendes IPsec-Protokoll.
Auf einem Windows-PC übernimmt die WINSOCK.DLL (oder WSOCK32.DLL) die Abwicklung der beiden Protokolle.
(→ Datagramm)

VPN (Virtuelles Privates Netzwerk)

Ein **V**irtuelles **P**rivates **N**etzwerk (VPN) schließt mehrere voneinander getrennte private Netzwerke (Teilnetze) über ein öffentliches Netz, z. B. das Internet, zu einem gemeinsamen Netzwerk zusammen. Durch Verwendung kryptographischer Protokolle wird dabei die Vertraulichkeit und Authentizität gewahrt. Ein VPN bietet somit eine kostengünstige Alternative gegenüber Standleitungen, wenn es darum geht, ein überregionales Firmennetz aufzubauen.

8 Technische Daten

CPU	Intel IXP 42x mit 266 MHz (bzw. 533 MHz Protector L)
Speicher	16 MB Flash, 32 MB SDRAM (bzw. 64 MB SDRAM Protector L)
LAN u. WAN Schnittstellen	Ethernet IEEE 802 10/100 Mbps RJ45
Stromversorgung	Via USB-Schnittstelle (5 V, 500 mA) oder durch externes Netzteil (110 - 230 V)
Betriebssystem	Innominate Embedded Linux
Funktionsüberwachung	Watchdog und optische Anzeige
Umwelt	Relative Luftfeuchtigkeit: max 90 %
	Temperatur: 0° bis 40°