

NAS absichern

Wenn Ihr NAS auch über das Internet erreichbar ist, dann sollten Sie es gegen Angriffe absichern. Das meiste lässt sich mit wenigen Mausklicks direkt auf der Bedienoberfläche erledigen.

Der Reiz eines NAS-Servers liegt unter anderem darin, dass sich die Inhalte jederzeit über das Internet nutzen lassen. So hören Sie etwa die Musik auf dem NAS mit dem Smartphone, sehen sich Fotos oder Filme an und greifen auf beliebige Daten zu.

Die Kehrseite: Auch Angreifer könnten versuchen, Zugang zu Ihrem NAS zu erhalten. Das geschieht oft mit automatischen Port-Scannern oder mit Brute-Force-Attacken, die Ihre Passwörter zu entschlüsseln versuchen.

Weil häufig wichtige Daten auf dem NAS liegen, etwa die Zugangsdaten fürs Online-Banking, sollten Sie Ihr NAS abschotten. Schon wenige einfache Tricks lassen einen großen Teil der Angriffe wirkungslos abprallen.

Der Artikel erklärt am Beispiel der NAS-Betriebssysteme Synology Diskstation Manager 5.0 und Qnap QTS 4.1.0, wie Sie Ihr NAS sicher machen. Bei NAS-Systemen anderer Hersteller funktioniert es meist entsprechend.

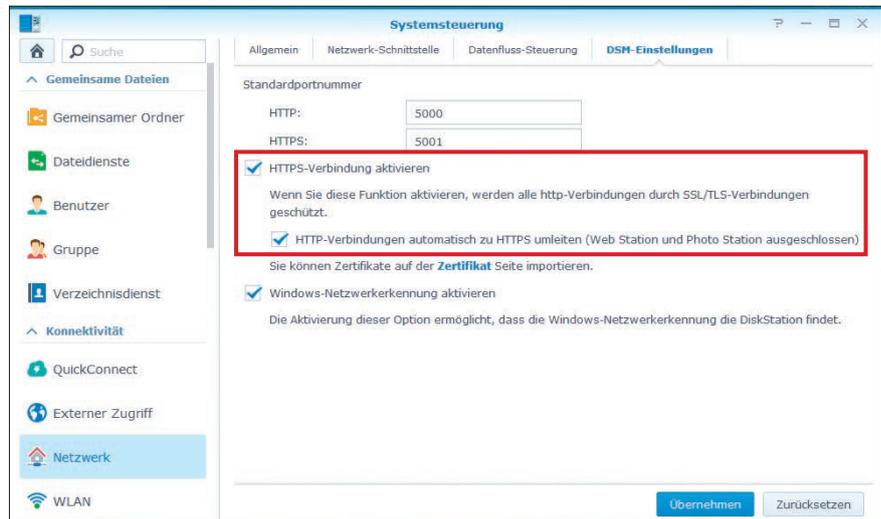
Ports

Um die diversen Programme auf dem NAS auch über das Internet zu nutzen, müssen Sie im Router eine Reihe von

Inhalt

NAS absichern

- **Ports**
 - HTTP verschlüsseln S. 80
 - SSH-Port ändern S. 81
 - WebDAV und Netdrive S. 81
 - Port-Tabelle S. 82
- **IP-Sperre** S. 82
- **Konten und Rechte** S. 82
- **Sicheres FTP** S. 83



Verbindungen verschlüsseln: Mit diesen Einstellungen verwendet Ihr Synology-NAS immer das verschlüsselte HTTPS-Protokoll (Bild A)

Ports öffnen. Geöffnete Ports sind ein beliebtes Einfallstor für Übelgesinnte. Wenn Sie die Standard-Ports ändern, sind bereits viele Angriffstechniken ausgehebelt.

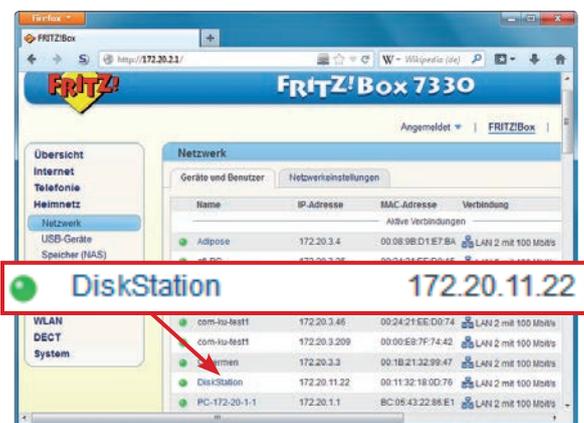
HTTP verschlüsseln

Beim Zugriff auf die Bedienoberfläche des NAS-Betriebssystems kommt standardmäßig das unverschlüsselte Protokoll HTTP über Port 80 zum Einsatz. Sicherer ist es, auf das verschlüsselte HTTPS umzustellen, das bei Synology den Port 5001 und bei Qnap den Port 8081 verwendet.

Für die Umstellung rufen Sie im Synology Diskstation Manager die Systemsteuerung auf und wählen dort „Netzwerk“. Im Reiter „DSM-Einstel-

lungen“ finden Sie die gesuchten Optionen. Setzen Sie jeweils ein Häkchen vor „HTTPS-Verbindung aktivieren“ und „HTTP-Verbindungen automatisch zu HTTPS umleiten (...)“ (Bild A).

Im QTS von Qnap rufen Sie ebenfalls die Systemsteuerung auf. Hier wechseln Sie zu „Allgemeine Einstellun-



IP-Adresse ermitteln: Die IP-Adresse Ihres NAS finden Sie bei der Fritzbox unter „Heimnetz, Netzwerk“ (Bild B)

gen“. Im Reiter „Systemadministration“ setzen Sie ein Häkchen vor „Nur eine sichere Verbindung (SSL) herstellen“.

Nun erfolgt der Zugriff auf das NAS-Betriebssystem stets verschlüsselt. Im Heimnetz ist dies zwar nicht nötig, schadet aber auch nicht.

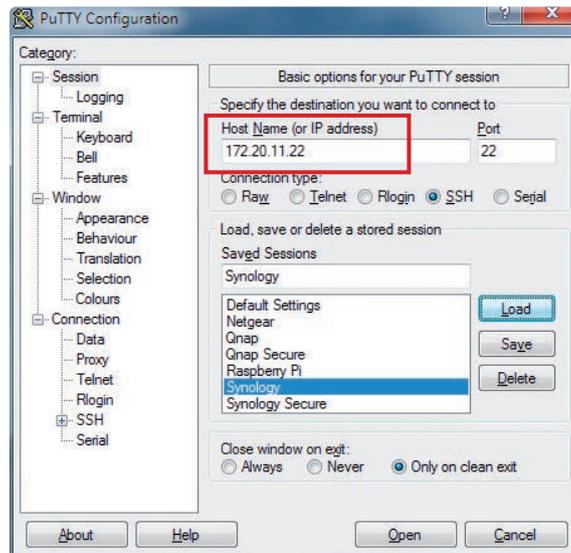
SSH-Port ändern

Ein beliebtes Angriffsziel auf NAS-Servern ist der SSH-Zugang. Damit gelangen Sie auf die Kommandozeilebene des NAS-Betriebssystems. Der Standard-Port für SSH ist 22. Wenn Sie diesen beispielsweise auf 604 ändern, dann laufen die Angriffe ins Leere.

Allerdings lässt sich der SSH-Port nicht im Webinterface ändern, sondern nur auf der Kommandozeile selbst. Außerdem gelingt dies nur auf NAS-Servern von Synology. Auf Qnap-NAS-Systemen werden die SSH-Konfigurationsdateien bei jedem Neustart überschrieben.

Installieren Sie zunächst unter Windows den SSH-Client Putty 0.63 (kostenlos, www.chiark.greenend.org.uk/~sgtatham/putty/download.html und auf ) . Nun benötigen Sie die IP-Adresse des NAS-Systems. Sie finden sie etwa im Webinterface Ihres Routers (Bild B) oder auf dem Synology-NAS im Widget „Systemzustand“ auf der rechten Seite. Die ermittelte IP-Adresse tragen Sie in Putty in das Feld „Host Name (or IP address)“ ein (Bild C).

Klicken Sie auf „Open“. Nun loggen Sie sich auf Ihrem NAS ein. Der Benutzername ist `root`, das Passwort Ihr Admin-Passwort. Geben Sie den Befehl `vi/etc/ssh/sshd_config` ein. `vi` ist ein einfacher Texteditor. Gehen Sie zu Zeile 13, in der `#Port 22` steht. Drücken Sie die Taste [I], um in den Eingabemodus zu gelangen. Entfernen Sie das `#` und ändern Sie die Port-Nummer, etwa in `604`. Drücken Sie [Esc], gefolgt von `:wq`, um `vi` wieder zu verlassen. Dann geben Sie `exit` ein, um die SSH-



Putty 0.63: Mit dem SSH-Client loggen Sie sich auf der Kommandozeilebene Ihres NAS ein. Tragen Sie hier dessen IP-Adresse ein (Bild C)

Sitzung zu beenden. Die Änderung des Ports greift erst nach einem Neustart.

WebDAV und Netdrive

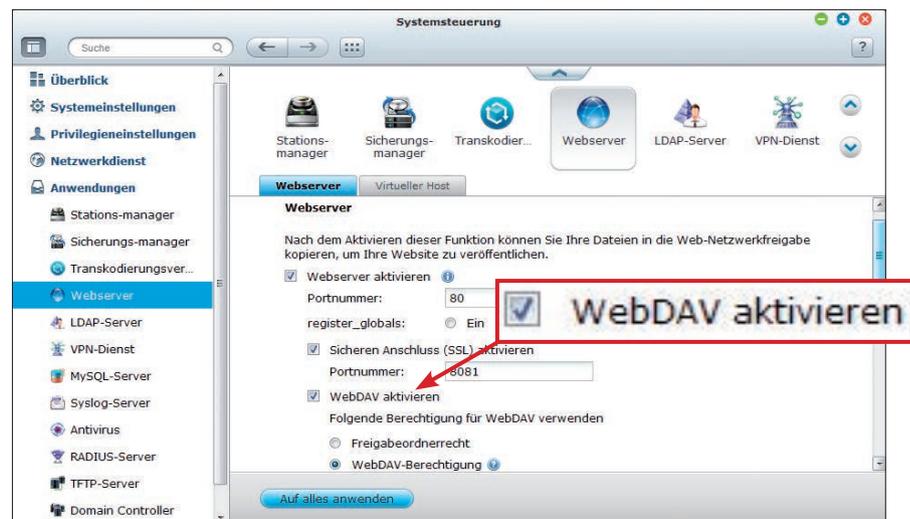
WebDAV steht für Web-based Distributed Authoring and Versioning und ist eine Erweiterung von HTTP. Wenn der WebDAV-Dienst aktiviert ist, lassen sich mit einem WebDAV-Client wie Netdrive 1.3.0.4 alle freigegebenen Ordner auf dem NAS als lokales Laufwerk in Windows einbinden (kostenlos, www.netdrive.net/old_versions.html und auf ) . Auch hier ist es sinnvoll, verschlüsselte Verbindungen zu wählen.

Die sicherste Variante ist natürlich, WebDAV zu deaktivieren. Wenn Sie aber auf WebDAV nicht verzichten wollen, dann machen Sie die Schotten dicht.

Im Diskstation Manager finden Sie die entsprechenden Optionen in der Systemsteuerung unter „Dateidienste, WebDAV“. Setzen Sie ein Häkchen vor „WebDAV HTTPS-Verbindung aktivieren“. Belassen Sie den Port auf 5006 und klicken Sie auf „Übernehmen“.

Im QTS klicken Sie in der Systemsteuerung auf „Webserver“. Setzen Sie Häkchen vor „Sicheren Anschluss (SSL) aktivieren“ und „WebDAV aktivieren“. Hier ist der voreingestellte verschlüsselte Port 8081 (Bild D).

So richten Sie Netdrive sicher ein: Klicken Sie nach der Installation des Tools auf „New Site“ und füllen Sie die Felder aus: Bei „Site-Name“ vergeben Sie einen beliebigen Namen. In das Feld „Site-IP oder URL“ tragen Sie die IP-Adresse oder den Hostnamen Ihres NAS ein, etwa `DiskStation`. Bei „Port“ tragen Sie für Synology `5006` und für Qnap `8081` ein. Als „Servertyp“ stellen Sie „WebDAV“ ein. Daneben geben Sie den gewünschten Laufwerkbuchstaben an. „Account“ und „Password“ sind Ihre Zugangsdaten zum ▶



WebDAV: Hier schalten Sie WebDAV bei einem Qnap-NAS ein (Bild D)

NAS. Nun klicken Sie auf „Advanced“ links unten und setzen ein Häkchen vor „Use HTTPS“. Ein Klick auf „Connect“ stellt die Verbindung her (Bild E).

Mit Hilfe einer DynDNS-Adresse ist dies auch über das Internet möglich. Mehr dazu lesen Sie im Artikel „Web-DAV – Tipps & Tricks“ in com! 7/2012 auf Seite 114 (kostenlos, www.com-magazin.de/33598).

Port-Tabelle

Um die Dienste eines NAS über das Internet zu nutzen, müssen die Ports für eingehende Daten teilweise vom Router an die interne IP-Adresse des NAS weitergeleitet werden.

Auf der Webseite www.synology-wiki.de/index.php/Zugriff_auf_die_Synology-Dienste_über_Internet finden Sie eine Übersicht der Ports, die von Synology-NAS-Systemen genutzt werden. Die rot hinterlegten Ports sollten auf jeden Fall geschlossen bleiben (Bild F).

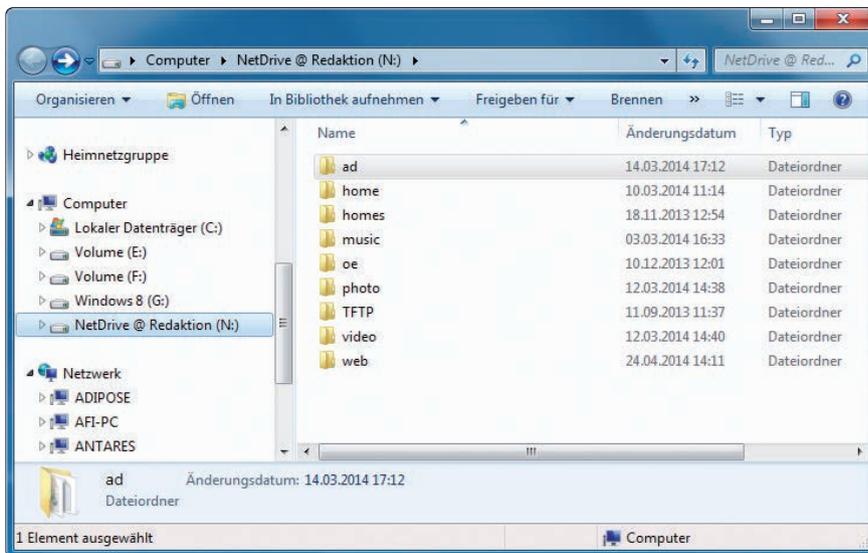
Für Qnap-NAS-Systeme finden Sie eine entsprechende Übersicht auf der Webseite <http://helpdesk.qnap.com/index.php?/Knowledgebase/Article/View/13/5/what-is-the-port-number-used-by-qnap--nas>.

IP-Sperre

Die häufigste Angriffsmethode auf NAS-Server nennt sich Brute Force. Dabei werden einfach unzählige Passwörter durchprobiert, bis eines passt.

Mit einer einfachen Einstellung lässt sich dem ein Riegel vorschieben: Nach einer bestimmten Anzahl von fehlgeschlagenen Login-Versuchen sperrt das Betriebssystem die dazugehörige IP-Adresse des Angreifers. Die Sperre lässt sich auf Wunsch nach einigen Tagen wieder aufheben.

Auf NAS-Systemen von Synology wählen Sie dazu



Netzlaufwerk: Das Tool Netdrive 1.3.0.4 bindet die freigegebenen Ordner auf dem NAS als Laufwerk unter Windows ein (Bild E)

in der Systemsteuerung den Eintrag „Sicherheit“. Im Reiter „Automatische Blockierung“ setzen Sie ein Häkchen vor „Automatische Blockierung aktivieren“. Darunter bestimmen Sie die Anzahl der fehlgeschlagenen Anmeldeversuche und die Zeitspanne, nach der eine Sperre erfolgen soll. Sinnvoll sind etwa 5 fehlgeschlagene Versuche in 3 Minuten. Optional lässt sich auch festlegen, nach wie vielen Tagen die Sperre wieder aufgehoben werden soll.

Dazu aktivieren Sie die Option „Verfahren der Blockierung aktivieren“.

Bei Qnap-NAS-Systemen rufen Sie ebenfalls in der Systemsteuerung „Sicherheit“ auf. Dort setzen Sie im Reiter „Netzwerkzugangsschutz“ ein Häkchen vor „Netzwerkzugangsverbindung aktivieren“. Darunter lässt sich detailliert festlegen, welche Zugriffsarten blockiert werden sollen. So lassen sich für SSH, FTP und HTTP unterschiedliche Bedingungen definieren.

In diesem Zusammenhang lohnt es sich auch, ab und zu einen Blick in die Systemprotokolle zu werfen. Dort finden Sie Informationen zu fehlgeschlagenen Anmeldeversuchen. Bei Synology sind die Protokolle im Protokoll-Center zu finden, bei Qnap in der Systemsteuerung unter „Systemprotokolle“ (Bild G).

Port	Protokoll	Beschreibung	Freigabe im Router für
20	TCP	aktiv FTP	Aktiv FTP
21	TCP	FTP-Control	FTP
22	TCP	SSH	SSH / verschlüsseltes Netzwerkbackup
23	TCP	Telnet	Telnet
25	TCP	SMTP (Mail)	Postfix (SMTP) Server der Mailstation
53	UDP/TCP	Domain Name Service	
67	UDP	DHCP Client	
80	TCP	HTTP	Web Station / Photo Station / Blog
110	TCP	POP3 (Mail)	Dovecot POP3 Server der Mailstation
123	UDP	Network Time Protocol	
137	UDP	NetBIOS	

Port-Tabelle: Die Seite www.synology-wiki.de/index.php/Zugriff_auf_die_Synology-Dienste_über_Internet zeigt, welche Ports geschlossen bleiben sollten (Bild F)

Konten und Rechte

Bei den Benutzerkonten, bei der Rechtevergabe und bei den Passwörtern

sollten Sie sehr sorgfältig vorgehen. Auch wenn Sie das NAS allein nutzen, ist es sinnvoll, neben dem Admin-Konto mehrere Benutzerkonten mit eingeschränkten Rechten einzurichten. Sie laufen dann nicht Gefahr, aus Versehen Daten zu löschen. Und wenn die Kontodaten an Fremde gelangen, können diese auch nur wenig Schaden anrichten. Das Admin-Konto sollten Sie möglichst ausschließlich zur Verwaltung verwenden. Zudem empfiehlt es sich, den Benutzer „guest“ zu deaktivieren.

Bei Synology finden Sie in der Systemsteuerung den Button „Benutzer“. Hier nehmen Sie alle relevanten Einstellungen vor. Über „Bearbeiten“ gelangen Sie zu den Berechtigungen. Hier legen Sie Schreib-, Lese- und Zugriffsrechte für die freigegebenen Ordner fest. Im Reiter „Applikationen“ bestimmen Sie, welche Programme der Benutzer ausführen darf. Unter „Erweitert“ lassen sich Regeln für Passwörter festlegen, etwa eine Mindestlänge oder zwingende Sonderzeichen.

Auch bei Qnap-NAS-Systemen gibt es in der Systemsteuerung den Button „Benutzer“. Zu jedem Benutzer finden Sie bei „Aktion“ die Buttons „Private Netzwerkfreigabe“ und „Applikations-

Typ	Datum	Uhrzeit	Benutzer	Quellen-IP	Computername	Inhalt
!	2014-04-25	12:07:16	System	127.0.0.1	localhost	[Security] Access Violation from 183.250.44.221 with TCP (port=23)
!	2014-04-25	12:07:16	System	127.0.0.1	localhost	Add IP: [183.250.44.221] to ban list for 1 day.
!	2014-04-25	12:04:30	System	127.0.0.1	localhost	[Security] Access Violation from 122.226.12.58 with TCP (port=23)
!	2014-04-25	12:04:30	System	127.0.0.1	localhost	Add IP: [122.226.12.58] to ban list for 1 day.
!	2014-04-25	08:53:09	System	127.0.0.1	localhost	[Media Library] Media Library Server started.
!	2014-04-25	08:52:21	System	127.0.0.1	localhost	System started.
!	2014-04-24	18:31:36	System	127.0.0.1	localhost	System was shut down on Thu Apr 24 18:31:36 CEST 2014.
!	2014-04-24	16:28:57	System	127.0.0.1	localhost	[Media Library] Media Library Server started.
!	2014-04-24	16:28:10	System	127.0.0.1	localhost	System started.
!	2014-04-24	16:25:06	System	127.0.0.1	localhost	System was shut down on Thu Apr 24 16:25:06 CEST 2014.
!	2014-04-24	16:23:31	admin	172.20.3.207	---	[Power Management] System will be restart now.

Systemprotokolle: Hier sehen Sie am Beispiel eines NAS-Systems von Qnap gescheiterte Angriffsversuche. Sie sind orange hervorgehoben (Bild G)

recht“. Ersterer bestimmt die Zugriffsrechte auf Ordner, letzterer die Ausführrechte für Programme und Dienste.

Sicheres FTP

Datenverkehr per FTP ist standardmäßig unverschlüsselt. Sogar der Benutzername und das Passwort werden im Klartext übertragen. Deshalb ist FTP anfällig für Lauschangriffe.

Am besten erlauben Sie nur verschlüsselte SSL/TLS-Verbindungen,

auch FTPES genannt. FTPES ist eine Untergruppe von FTPS, wobei das E für explizit steht.

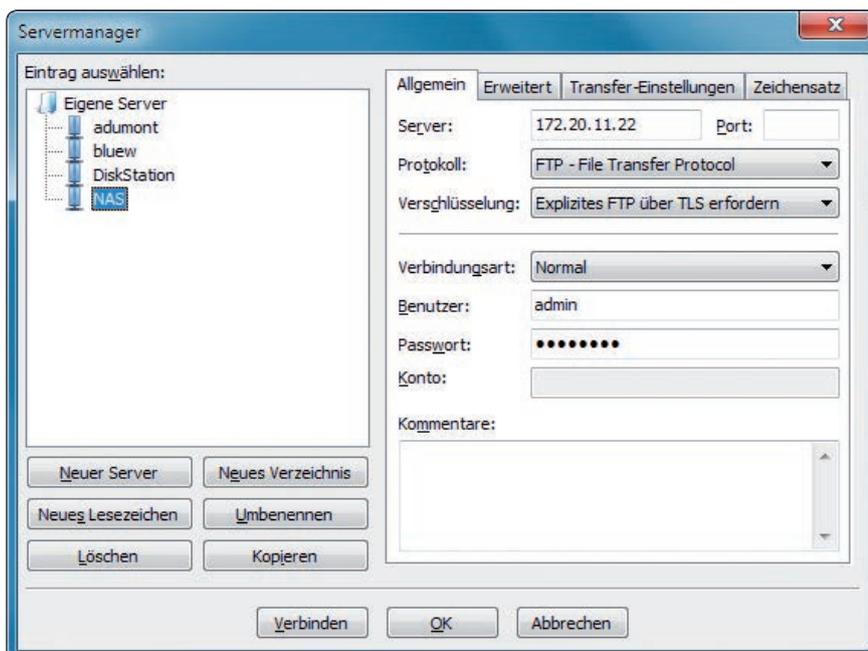
Klicken Sie im Synology Diskstation Manager in der Systemsteuerung auf „Dateidienste“ und wechseln Sie dort in den Reiter „FTP“. Setzen Sie ein Häkchen vor „FTP SSL/TLS Verschlüsselungsdienst (FTPS) aktivieren“ und entfernen Sie das Häkchen vor „FTP-Dienst aktivieren (keine Verschlüsselung)“.

Qnap QTS hat in der Systemsteuerung einen Button „FTP“. Hier setzen Sie Häkchen bei „FTP-Dienst aktivieren“ und „FTP mit SSL/TLS (explizit)“.

Im FTP-Client, etwa Filezilla, stellen Sie im Feld „Verschlüsselung“ dann „Explizites FTP über TLS erfordern“ ein (Bild H). Bei der ersten Verbindung erhalten Sie vom FTP-Client eine Meldung bezüglich des verwendeten Zertifikats. Bestätigen Sie es mit „OK“.

Mehr zu FTP lesen Sie im Artikel „FTP mit Filezilla Client und Server“ in com! 10/2013 auf Seite 24 (kostenlos, www.com-magazin.de/115076). ■

Andreas Dumont
computer@com-magazin.de



Sicheres FTP: So stellen Sie den FTP-Client Filezilla ein, um verschlüsseltes FTP zu gewährleisten (Bild H)

Weitere Infos

- www.com-magazin.de/33294
Artikel und Tipps zum Thema NAS