



# NETGEAR

Everybody's connecting.

## FAQ FVS318

Die meistgestellten Fragen zum  
**FVS318 xDSL/Kabel VPN Router**

### 1 Was ist ein FVS318 xDSL/Kabel VPN Router?

FVS318 ist ein Netzwerk-Sicherheitsgerät, um mehrere PCs (Local Area Network – LAN) in einem kleinen Büro mit dem Internet (Wide Area Network – WAN) auf sichere Weise zu verbinden. Und das auf sichere Weise über eine einer Breitband-Modemverbindung wie xDSL oder Kabelmodem.

### 2 Ist es ein Router?

Ja, es ist ein Router und noch viel mehr. Der FVS318 stellt alle Funktionalitäten eines NAT (Network Address Translation) Routers bereit und zusätzlich noch viele Sicherheitsfunktionen.

### 3 Welche besonderen Merkmale hat der FVS318?

Der FVS318 sorgt für zusätzliche Sicherheit im Netzwerk, da er vier zusätzliche wichtige Leistungsmerkmale bereitstellt, die in einem konventionellen NAT-Router nicht existieren:

- VPN Endpunkt-Support mit IPSec 3DES Verschlüsselungsmöglichkeit.
- Statische Content (Inhalt) Filterung (URL, URL Schlüsselwörter)
- Abweisung von DoS (Denial of Service), Vorbeugung durch genaue Datenpaket-Kontrolle.
- Logging, Reporting und Alarm-Meldungen (Intrusion Detection System)

### 4 Was ist der Unterschied zwischen dem FVS318 und dem von NETGEAR vorher ausgelieferten FV318?

Der FVS318 hat neue Leistungsmerkmale, mit welchen er eine bessere Performance und ein besseres Preis-Leistungsverhältnis erreicht.

Die Spezifikationen des FVS318 sind:

- Keine Benutzer-Limitierung der Firewall
- Unterstützt 8 VPN Tunnels (FV318 unterstützt bis zu 5)
- Ein verbessertes Benutzer-Interface für einen schnelleren Netzwerkzugriff und bessere Performance
- Eines der niedrigsten Preis-pro-Port-Verhältnisse im Vergleich mit den meisten VPN Produkten am Markt.

**NETGEAR Deutschland GmbH**

Konrad-Zuse-Platz 1 • 81829 München • GERMANY

Tel.: +49 (0)89 / 9 27 93 - 25 00 • Fax: +49 (0)89 / 9 27 93 - 25 10

<http://www.netgear.de>



# NETGEAR

Everybody's connecting.

- Die Kompatibilitätsliste mit anderen VPN Produkten auf dem Markt wurde erweitert.

## 5 Was ist ein "Virtual Private Network"?

Allgemein bekannt als VPN wird es aber in verschiedenen Publikationen auf verschiedene Art definiert. Beschrieben wird damit eine Gruppe von zwei oder mehreren Computersystemen, typischerweise zu einem privaten Netzwerk (ein Netzwerk, dass von einer Organisation ausschließlich für die eigene Benutzung aufgebaut und betrieben wird) verbunden, welches einen limitierten Zugang zu öffentlichen Netzwerk hat. Die Kommunikation zu einem öffentlichen Netzwerk wie zum Beispiel das Internet erfolgt „sicher“ über einen VPN-Tunnel. VPNs können zwischen einem individuellen Computer und einem privaten Netzwerk oder zwischen einem privaten Netzwerk (Server-to-Server) und einem entfernten LAN bestehen. Sicherheitsmerkmale unterscheiden sich von Produkt zu Produkt, aber die meisten Sicherheits-Experten sind sich darüber einig, dass VPNs strenge Authentifizierung von extern angebenen Benutzern und Servern, Verschlüsselung und Mechanismen zum verstecken und maskieren von Informationen über die private Netzwerk-Topologie gegen potentielle Attacken aus dem öffentlichen Netzwerk beinhalten müssen.

## 6 Was ist "VPN End Point" (Endpunkt) und was kann es?

Die "VPN End Point" Fähigkeit in einem Router ermöglicht es, einen VPN-Tunnel zu einem anderen Punkt aufzubauen, welcher ebenfalls einen VPN-Client (Client-to-Box) unterstützt oder ebenfalls über die VPN End point Fähigkeit (Box-to-Box) verfügt.

## 7 Wie viele VPN Tunnels kann der FVS318 zu gleicher Zeit unterstützen?

Der FVS318 hat als Standard die Möglichkeit, bis zu 8 VPN Tunnels zu gleicher Zeit zu unterstützen. Dies kann sowohl eine Kombination aus Zweigniederlassung, mobilen Benutzern oder Verbindung zu einem Partner sein.

## 8 Was ist Encryption (Verschlüsselung)?

Es ist eine mathematische Rechenoperation, welche die Daten von einem "klaren Text" in einen "chiffrierten Text" umwandelt, der nicht ausgelesen werden kann. Normalerweise benötigt der mathematische Rechenprozess einen alphanumerischer Schlüssel, der mit dem "Klartext" mitgeliefert wird. Der Klartext und der Schlüssel laufen dann durch einen Verschlüsselungsprozess, welcher die Daten zerstückelt und durcheinander mixt und sie damit sicher macht. Bei der Entschlüsselung geschieht der umgekehrte Prozess wie bei der Verschlüsselung, die Daten werden ebenfalls durch eine mathematische Rechenoperation von dem verschlüsselten Text wieder in einen Klartext umgewandelt.

**NETGEAR Deutschland GmbH**

Konrad-Zuse-Platz 1 • 81829 München • GERMANY

Tel.: +49 (0)89 / 9 27 93 - 25 00 • Fax: +49 (0)89 / 9 27 93 - 25 10

<http://www.netgear.de>



# NETGEAR

Everybody's connecting.

## 9 Wie werden die Daten in dem VPN verschlüsselt?

Die Daten werden per Software verschlüsselt, dadurch werden zusätzliche Kosten für einen teureren Co-Prozessor vermieden.

## 10 Was bedeutet DES oder 3DES?

DES steht für "Digital Encryption Standard". Hier wird die Verschlüsselung für Datenverkehr benützt, bei dem Sender und Empfänger den selben Sicherheitsschlüssel besitzen müssen. Dieser kann dann dazu benützt werden, um Nachrichten zu verschlüsseln und wieder zu entschlüsseln oder um einen Berechtigungscode zu generieren und verifizieren. NETGEAR DES-Verschlüsselung benützt einen 64-bit Schlüssel. 3DES, oder "triple-DES", ist im Unterschied dazu eine Variation von DES, welche einen 168-bit Schlüssel verwendet, um für den Datenverkehr mehr Sicherheit als DES zu generieren. DES3 wird von Sicherheitsexperten als virtuell nicht durchdringbar angesehen. Es benötigt allerdings auch erheblich mehr Prozessorleistung, was zu erhöhten Verzögerungen und geringerem Datendurchsatz führt.

## 11 Was ist IKE?

IKE steht für "Internet Key Exchange" (Internet Schlüssel Austausch) und ist ein Protokoll zum Austausch der Schlüssel, spezifiziert von der IETF (Internet Engineering Task Force). Eine IKE SA (Security Association) übernimmt automatisch die Verschlüsselungsübertragung und den Berechtigungscode. IKE wird bei Übertragungsbeginn aktiviert und bestätigt die VPN Session und vermittelt automatisch die Schlüssel, welche dann für den IP-Verkehr benützt werden.

## 12 Was ist eine SA (Security Association)?

SA ist eine Gruppe von Sicherheitseinstellungen, die sich auf einen bestimmten VPN-Tunnel beziehen. Eine SA umfasst alle notwendigen Einstellungen, um einen VPN-Tunnel zu generieren. Verschiedene SAs können erstellt werden, um Zweigniederlassungen anzubinden, um sicheres Remote Management zu erlauben und nicht unterstützten Datenverkehr weiterzuleiten. Alle SAs benötigen eine spezifische Verschlüsselungsmethode, eine IPSec-Gateway-Adresse und eine Ziel-Netzwerkadresse. IKE beinhaltet einen gemeinsamen Geheimcode.

## 13 Was ist PPTP?

"Point-to-Point Tunneling Protocol" setzt auf die Funktionalitäten des Point-to-Point Protocols auf und ermöglicht eine Einwahl von außen, die durch das Internet zu einer bestimmten Zieladresse oder einem Computer getunnelt wird. PPTP benützt das GRE

**NETGEAR Deutschland GmbH**

Konrad-Zuse-Platz 1 • 81829 München • GERMANY

Tel.: +49 (0)89 / 9 27 93 - 25 00 • Fax: +49 (0)89 / 9 27 93 - 25 10

<http://www.netgear.de>



# NETGEAR

Everybody's connecting.

(Generic Routing Encapsulation) Protokoll, um PPP Pakete einzukapseln. Das gibt PPTP die Flexibilität, auch mit anderen Protokollen als IP zu arbeiten.

## 14 Was ist IPSec?

IPSec steht für "Internet Protocol Security" und ist ein robuster VPN Standard, der die Berechtigungen und die Verschlüsselungen für den Datenverkehr über das Internet abdeckt. Die VPN-Technologie mit eingebundener IPSec verschlüsselt alle ausgehenden Daten und entschlüsselt alle eingehenden Daten, so dass öffentliche Netze wie das Internet als sicheres Transportmedium genutzt werden können. IPSec unterstützt zwei verschiedene Verschlüsselungsarten: Transport und Tunnel. Die Transportfunktion verschlüsselt den Datenanteil von jedem Datenpaket, belässt aber den Header (Kopf des Datenpakets, enthält Quell- und Zieladresse und Steuerinformationen) unverschlüsselt. Die sicherere Methode ist die Tunnelfunktion. Sie verschlüsselt beides, den Header und den Datenblock. Auf der Empfängerseite entschlüsselt ein dem IPSec Standard entsprechendes Gerät jedes Datenpaket wieder. IKE Protocol ist ein wichtiger Management Protokoll Standard und wird im Allgemeinen in Verbindung mit IPSec benutzt. Im Unterschied zu PPTP unterstützt IPSec nur IP und bietet keine Sicherheit für andere Protokolle. PPTP unterstützt zwar verschiedene Protokolle, bietet dafür aber keine Sicherheit.

## 15 Warum benötige ich einen Router, wenn mein Computer bereits über einen Zugang zum Internet verfügt?

Fälle von Computerkriminalität haben einen rasanten Zuwachs und Angriffe von Hackern auf Firmennetzwerken und private Computer gehören zu den täglichen Nachrichten. Die Abhängigkeit von Computern, auf denen wichtige Daten gespeichert sind und die Entwicklung von Softwareanwendungen, die über das Internet auf gemeinsame Daten zugreifen, lassen Netzwerksicherheit zu einem sehr wichtigen Thema werden. Die einfache Verbindung eines Computers zum Internet mit xDSL-Modem oder Kabelmodem bietet keinerlei Sicherheit, um einen Hackerangriff abzuwehren. Wohingegen ein Router, der NAT (Network Address Translation) unterstützt, dieses Problem ganz einfach löst.

## 16 Was bedeutet NAT (Network Address Translation)?

NAT ersetzt die "private" IP-Adresse von Geräten auf der lokalen LAN-Seite des Routers durch eine neue "öffentliche" IP-Adresse, die der Router nach außen, z.B. zum Internet, weitergibt. Das heißt, nur die IP Adresse des Routers ist nach außen sichtbar. Mit diesem einfachen, aber effizienten, Verfahren können alle Geräte in diesem LAN (bis zu 253) versteckt oder ‚maskiert‘ werden. Es kann dadurch kein einzelner spezifischer PC mehr von außen lokalisiert werden. Diese Technologie bietet simplen Schutz gegen Hackerangriffe und wird weit verbreitet in Breitband-Routern benutzt.

**NETGEAR Deutschland GmbH**

Konrad-Zuse-Platz 1 • 81829 München • GERMANY

Tel.: +49 (0)89 / 9 27 93 - 25 00 • Fax: +49 (0)89 / 9 27 93 - 25 10

<http://www.netgear.de>



# NETGEAR

Everybody's connecting.

## 17 Ist es das gleiche wie eine Firewall?

Nein. Die Bezeichnung "Firewall" wurde generell benutzt, um die Fähigkeit des Routers zu beschreiben, die lokalen IP-Adressen zu maskieren. Eine echte Firewall beinhaltet auch eine weitere Technologie, die SPI (Stateful Packet Inspection). Firewalls bieten einen höheren Stand an Sicherheit, sind aber auch generell teurer als ein NAT-Router. Bei Firewalls hat der Administrator verschiedene Einstellmöglichkeiten, zum Beispiel den Zugriff auf bestimmte IP-Adressen oder Domain-Namen zu erlauben und andere abzuweisen (Filtering). Firewalls können ebenso den externen Zugriff auf das private Netzwerk regeln. Dies geschieht durch die Verwendung von sicheren Login-Prozeduren und Berechtigungszertifikaten (VPNs – Virtual Privat Networks). Firewalls werden dazu benutzt, um DoS-Attacken abzuwehren und können per Software Inhalte filtern, um den Zugriff auf unerwünschte Webseiten zu unterbinden. Es gibt auch umfangreiche Reporting-Möglichkeiten, bekannt als "Intrusion Detection System". Der FVS318 ist eine echte Firewall.

## 18 Was ist SPI (Stateful Packet Inspection)?

SPI ist eine Technologie, die in Firewalls verwendet wird. Anstatt die IP- Adresse einfach nur zu verstecken, durchsucht SPI jedes einzelne Datenpaket nach Informationen wie seinem Ursprung und seiner Zieladresse und des Protokolls, das benutzt wird. Nach einer Reihe von vorher eingestellten Kriterien kann SPI dann entsprechende Maßnahmen ergreifen. Da SPI den Inhalt des Pakets filtert, kann es auch vor DoS-Attacken schützen.

## 19 Was sind DoS (Denial of Service) Attacken?

Pakete oder Serviceanfragen, die von einem oder mehreren PCs geschickt werden, können eine Funktionsstörung des Zielcomputers oder Servers auslösen. Ein Weg, um einen DoS einzusetzen ist, den Zielservers erbarmungslos anzupingen ("Ping of Death"), was diesem abverlangt, auf den Ping zu antworten. Wenn der Server mit ausreichend Pings attackiert wird, ist er nicht mehr in der Lage, auf all diese Pings zu reagieren und gleichzeitig andere Funktionen durchzuführen. Das Resultat ist ein DoS (Denial of Service – Verweigerung von Service).

## 20 Wie schützt SPI vor einem „Ping of Death“ oder einer SYN Flood Attacke?

Der Router prüft jedes Datenpaket und falls er bemerkt, dass eine bestimmte Anzahl von Pings über einen bestimmten Zeitraum von der gleichen Adresse angefordert werden, wird er diese Pakete einfach fallen lassen. In einem anderen Beispiel kommt es darauf an, dass der Router erkennt, ob die Ursprungsadresse innerhalb oder außerhalb des LANs liegt. Wenn eine Attacke aus dem WAN heraus gestartet wird und eine interne Ursprungsadresse in dem auslösenden Paket verwendet wird, wäre die normale Reaktion eines Routers, langsamer zu werden, da er nicht wüsste, wohin er die Antwort

**NETGEAR Deutschland GmbH**

Konrad-Zuse-Platz 1 • 81829 München • GERMANY

Tel.: +49 (0)89 / 9 27 93 - 25 00 • Fax: +49 (0)89 / 9 27 93 - 25 10

<http://www.netgear.de>



# NETGEAR

Everybody's connecting.

schicken soll. SPI Router sind in der Lage, den Herkunft von Paketen in der Relation zu vorhergehenden Paketen zu analysieren und feststellen, dass die Ursprungsadresse inkorrekt ist. Darauf hin wird das auslösende Packet fallengelassen und eine Verlangsamung des Netzwerks vermieden.

## 21 Was für verschiedene DoS Attacken gibt es?

- Solche, die fehlerhafte Datenpakete in die TCP/IP-Implementation einfügen, z.B. Ping of Death oder Teardrops.
- Solche, welche die Schwächen in der TCP/IP Spezifikation ausnützen wie zum Beispiel SYN Flood und LAN Attacks.
- Massive Attacken, die das Netzwerk mit nutzlosen Daten überschwemmen, z.B. Smurf Attack.
- IP Spoofing

## 22 Was für andere Sicherheitsfunktionen bekommen ich mit dem FVS318?

Zusätzlich zu den echten Firewall Funktionen wird der FVS318 mit folgender Software ausgeliefert: Freedom Anti-Virus und Privacy Software von Zero Knowledge System (ZFK). Die Software ist kostenlos und für ein Jahr gültig. Sie kann für Anwendungen für bis zu 8 PCs verwendet werden. Wenn Sie einen Upgrade für mehr als 8 PCs benötigen oder sich für weitere Sicherheitsfunktionalitäten von ZFK interessieren, finden Sie Details auf der Webseite [www.NETGEAR.com](http://www.NETGEAR.com).

## 23 Was ist "Content Filtering" (Content - Inhalt)?

Der Router besitzt die Möglichkeit, Benutzern den Zugang zu bestimmten Webseiten zu verweigern. Dies geschieht nach vorher festgelegten Regeln. Das ‚Content Filtering‘ kann auf verschiedene Arten durchgeführt werden. Einige der populäreren Wege beinhaltet das Filtern basierend auf die Web URL, Schlüsselwörter in der URL oder festgelegt auf bestimmte Tageszeiten oder Wochentage.

## 24 Filtert der FVS318 die Inhalte nach diesem Prinzip?

Ja. Das ist als Standard immer implementiert. Diese Art des Filtering ist auch bekannt als "Static Content Filtering".

## 25 Wie viele Benutzer werden vom FVS318 unterstützt?

Der FVS318 kann bis zu 253 Benutzer unterstützen.

## 26 Wo kann ich das Produkt kaufen?

**NETGEAR Deutschland GmbH**  
Konrad-Zuse-Platz 1 • 81829 München • GERMANY  
Tel.: +49 (0)89 / 9 27 93 - 25 00 • Fax: +49 (0)89 / 9 27 93 - 25 10  
<http://www.netgear.de>



# NETGEAR

Everybody's connecting.

Bezugsadressen für den FVS318 xDSL/Kabel VPN Router finden Sie auf der Web-Seite [www.NETGEAR.de](http://www.NETGEAR.de).

## 27 Welcher Prozessor wird im FVS318 verwendet?

Der FVS318 benützt einen 50 MHz ARM RISC Prozessor.

## 28 Wie viel Speicher besitzt der FVS318?

Der FVS3128 verfügt über 1MB Flash Memory und 16 MB DRAM Memory auf dem Board. Damit ist für mehr als genügend Platz für zukünftige Upgrade Funktionalitäten gesorgt.

## 29 Was für weitere Produkte benötige ich, wenn ich einen FSV318 einsetzen möchte?

Sie benötigen eine Ethernet Karte und eine Highspeed Breitband Internetverbindung (z.B. Kabel oder DSL).

## 30 Was ist, wenn ich einen VPN Tunnel zu einem anderen Standort aufbauen möchte?

Um einen VPN Tunnel aufzubauen, benötigen Sie folgendes:

- Ein Gerät, das einen VPN-Tunnel aufbauen kann, wie z.B. der FVS318.
- Entweder eine Client-Software für den mobilen Benutzer oder anderes Gerät, dass den TPN Tunnel terminieren kann wie z.B. ein weiterer FVS318. Sie können ebenfalls einen Router verwenden, der IPSec in Verbindung mit einer Client-Software (für sicheres Teilen der Verbindung auf der externen Seite) unterstützt.

## 31 Was ist, wenn ich mehrere VPN Standorte benötige?

Benützen Sie die selbe Vorgehensweise wie oben beschrieben. Benützen Sie für jede weitere Site die selbe Client-Software oder einen gleichen Firewall Router.

## 32 Welche VPN Client-Software wird vom FVS318 unterstützt?

Der FVS318 unterstützt den Safenet Client (Soft-PK, SoftRemote), dieser ist verfügbar auf der Webseite [www.safenet-inc.com](http://www.safenet-inc.com).

## 33 Was ist mit anderen VPN Clients?

NETGEAR wird Anwendungsbeschreibungen zum Einbinden von anderen VPN Clients (z.B. Microsoft, Checkpoint, etc.) zur Verfügung stellen, wenn die Tests und



# NETGEAR

Everybody's connecting.

Kompatibilitätsprüfungen abgeschlossen sind. Diese werden dann auf der NETGEAR Support Seite zur Verfügung gestellt. Diese Clients werden aber nicht von unserem Technischen Support Service unterstützt.

## **34 Was ist mit anderen VPN Geräten?**

Der FVS318 ist mit weiteren FVS318 auf Kompatibilität getestet worden und wird durch den Technischen Support unterstützt. Vieles, wie z.B. die VPN Client Software und Application Notes für andere VPN Hardware, wird auf die Technische Support Seite gestellt. Dafür kann allerdings nicht vom Technischen Support Service keine Unterstützung gegeben werden.

## **35 Kann ich einen weiteren VPN Router auf einer externen Seite einbinden, um noch mehr VPN-Tunnels zu anderen Punkten aufzubauen?**

Diese Technik, bekannt als "hub and spoke" VPN Methode, wird unterstützt, aber nur ein "hub and spoke" kann benützt werden. In diesem Falle ist es nicht möglich, einen weiteren „hub“ auf der externen Seite zu haben.

## **36 Welche Plattformen werden vom FVS318 unterstützt?**

Der FVS318 arbeitet auf Plattformen, auf denen das TCP/IP Protokoll eingebunden ist (wie z.B. Macintosh, Linux, Unix, etc.) und kann einen Browser benützen (wie Netscape und Windows IE).

## **37 Kann der FVS318 auch mit anderen als NETGEAR Netzwerkprodukten zusammen arbeiten?**

Natürlich funktioniert der FVS318 auch mit anderen Nicht-NETGEAR Netzwerkprodukten, wenn diese dem Ethernet Standard (802.3) entsprechen.

## **38 Wie einfach ist es, sich mit dem FVS318 ans Internet anzubinden?**

Sie können den FVS318 ganz einfach mit ihrem existierenden Web-Browser (z.B. Netscape oder Internet Explorer) aufsetzen. Verbinden Sie ganz einfach Ihr xDSL/Kabel-Modem mit dem WAN-Port auf der Rückseite des FVS318, verbinden Sie Ihre Computer mit den LAN Ports und dann konfigurieren Sie den FVS318, indem in der URL Adresszeile Ihres Webbrowsers die „192.168.0.1“ eingeben. Starten Sie nach dem Log-in dem SmartWizard und folgen Sie den Anweisungen. Bitte sehen Sie auch in das Benutzer-Handbuch für weitergehende Informationen.

**NETGEAR Deutschland GmbH**

Konrad-Zuse-Platz 1 • 81829 München • GERMANY

Tel.: +49 (0)89 / 9 27 93 - 25 00 • Fax: +49 (0)89 / 9 27 93 - 25 10

<http://www.netgear.de>



# NETGEAR

Everybody's connecting.

**39 Ich habe bereits eine 10 oder 100 MBit/s. Ethernet Karte, ist diese kompatibel mit dem FVS318?**

Ja, der FVS318 hat einen eingebauten Autosensing Switch, der sowohl 10 wie auch 100 MBit/s. unterstützt.

**40 Der FVS318 unterstützt "Auto Uplink". Was ist ein "Auto Uplink"?**

"Auto Uplink" ist die Fähigkeit der LAN-Ports am Firewall, die korrekte Verbindungsart zu ermitteln (entweder MDI oder MDI-X), wenn er mit einem anderen LAN-Gerät verbunden wird. Diese Funktionalität macht Cross-over-Kabel überflüssig. Auch braucht man keinen physikalischen Uplink-Schalter an dem LAN Gerät mehr. Das macht die Verbindung zu anderen Geräten viel einfacher.

**41 Arbeitet der FVS318 mit meinem bestehenden xDSL oder Kabel Internet Service zusammen?**

Der FVS318 sollte mit den meisten Service Providern zusammen arbeiten. Aber es gibt natürlich auch einige ISPs, für die man vielleicht eine spezielle Konfiguration benötigt (z.B. Host-Name, Domain-Name, etc.). Das Modem sollte einen Ethernet-Port für die Verbindung zum Router haben.

**42 Was ist der Unterschied zwischen einer statischen und einer dynamischen IP Adresse?**

Die statische IP-Adresse wird dem Kunden fest zugeschrieben, wenn er sich zum ersten Mal bei seinem Internet Service Provider anmeldet. Eine dynamisch vergebene IP-Adresse wird Ihnen vorübergehend zugewiesen, wenn Sie sich ins Internet einwählen. Diese Adresse hat ein vorher festgelegtes Zeitlimit.

**43 Wie kann ich mit dem FVS318 auf Internet-Spiele und Anwendungen (z.B. Napster, ICQ, AIM, etc.) zugreifen?**

Stellen Sie in der Web-Konfigurationsseite den Public Server (Port Forwarding) ein. Generell werden VPN-Produkte nicht für Internet-Spiele empfohlen, da die ganzen Sicherheitsprozeduren und die Verschlüsselung den Datenaustausch verlangsamen und das möglicherweise negative Effekte auf die Rückmeldungszeiten hat.

**44 Erlaubt der FVS318 auch einen „DMZ“?**

Ja, der FVS318 unterstützt auch einen ungeschützten Server, auch bekannt als DMZ. Das erlaubt Ihnen, ein Gerät wie zum Beispiel einen Web-Server oder einen für Spiele benützten PC, aus dem Firewall heraus zu setzen. Bitte sehen Sie ins Handbuch für detaillierte Anweisungen.

**NETGEAR Deutschland GmbH**

Konrad-Zuse-Platz 1 • 81829 München • GERMANY

Tel.: +49 (0)89 / 9 27 93 - 25 00 • Fax: +49 (0)89 / 9 27 93 - 25 10

<http://www.netgear.de>



# NETGEAR

Everybody's connecting.

## 45 Es ist mir nicht möglich, eine Web Konfigurations-Seite für den FVS318 zu bekommen. Was kann ich tun?

- Sie müssen möglicherweise die Proxy-Settings in Ihrem Internet Browser entfernen. Oder entfernen Sie die Dial-up Settings in Ihrem Browser.
- Der PC erhält möglicherweise keine IP-Adresse. Starten Sie Ihren PC neu und führen Sie `winiipcfg` aus (Windows ME und älter) oder `ipconfig` auf der Windows NT Plattform, um eine dynamische IP-Adresse zuzuweisen. Dann starten Sie denn Browser.

## 46 Was bedeutet PPPoE?

PPPoE steht für "Point to Point Protocol over Ethernet" und wurde von der PPP Arbeitsgruppe des IETF erarbeitet. PPPoE ist ein viel einfacherer Weg, um eine PPP-Verbindung über einen xDSL-Zugang für ein ans Ethernet angebundenes xDSL-Modem aufzubauen. Es nützt die Vorteile der geteilten Ethernet-Umgebung zugleich mit PPPs vertrautem und sicheren Dial-Access Benutzermodell.

Weitere Vorteile von PPPoE:

- Erlaubt einzelnen PCs, eine PPP Session zu verschiedenen Zielnetzwerken zur gleichen Zeit aufzubauen.
- Erlaubt es einem LAN und mehreren PCs, simultan PPP-Sessions zu verschiedenen Zielnetzwerken aufzubauen.

## 47 Ist es dem FVS318 möglich, VPN auch anders als durch VPN End-Point Möglichkeit zu unterstützen?

Ja, der FVS318 unterstützt VPN passiv durch IPsec und PPTP Pass-through.

## 48 Unterstützt der FVS318 auch Remote Management?

Ja, Remote Management kann über das Web durchgeführt werden. Sie können das Remote Management so einrichten, dass für jeden eine bestimmte Reihe von IP Adressen zur Verfügung steht oder eine spezifische IP Adresse, um remote ein bestimmtes Gerät zu managen. Stellen Sie sicher, dass sie für diese Funktion ein sicheres Passwort und Benutzernamen auswählen.

## 49 Unterstützt der FVS318 auch AppleTalk oder IPX?

Nein, der FVS318 unterstützt weder AppleTalk noch IPX.

## 50 Unterstützt der FVS318 auch NetBEUI?

Nein, der FVS318 unterstützt kein NetBEUI.



# NETGEAR

Everybody's connecting.

## 51 Unterstützt der FVS318 andere Betriebssysteme?

Ja, der FVS318 ist kompatibel zu anderen Betriebssystemen, vorausgesetzt dieses System unterstützt auch TCP/IP (wie zum Beispiel Web-Browser).

## 52 Wie setze ich Einschränkungen, welche Webseiten von Benutzern besucht werden dürfen?

Sie können dies in der FVS318 Konfiguration auf der "Content Filtering" Seite einstellen. Bitte lesen Sie das Handbuch, um eine detaillierte Beschreibung für diese Einstellungen zu bekommen.

## 53 Kann ich den werkseitig eingestellten Benutzernamen und Passwort ändern?

Ja, das sollten Sie auch unbedingt tun, um Ihren PC oder Ihr LAN abzusichern. Bitte lesen Sie auch hierzu das Handbuch, um eine detaillierte Beschreibung für die Änderung dieser Parameter zu bekommen.

## 54 Wie kann ich kontrollieren, ob meine Ports auch wirklich abgesichert sind?

Sie können das kontrollieren, indem Sie eine Scanning Utility Software einsetzen. Diese können Sie zum Beispiel unter folgenden Adressen finden: [www.grc.com](http://www.grc.com) oder [www.syngatetech.com](http://www.syngatetech.com).

## 55 Wie kann ich den Technischen Support von NETGEAR erreichen?

So können den Technischen Support von NETGEAR hier erreichen:

- Support Hotline in Deutschland: 0800-7 57 57 77
- Support Hotline in Österreich: 0800-20 23 12
- Support Hotline in der Schweiz: 0800-47 47 44
- Per Email über das Internet: <http://www.netgear.de/support/web-support.html>

## 56 Wie kann ich mehr über VPN erfahren?

Besuchen Sie unsere Web-Seite unter [www.netgear.com](http://www.netgear.com) und klicken Sie "Planet VPN" an.

**NETGEAR Deutschland GmbH**

Konrad-Zuse-Platz 1 • 81829 München • GERMANY

Tel.: +49 (0)89 / 9 27 93 - 25 00 • Fax: +49 (0)89 / 9 27 93 - 25 10

<http://www.netgear.de>



# NETGEAR™

Everybody's connecting.

© 2002 NETGEAR Deutschland GmbH.

Alle Rechte vorbehalten.

Eine Vervielfältigung, Reproduktion, Publikation oder Veröffentlichung ist nur mit ausdrücklicher, schriftlicher Genehmigung der NETGEAR Deutschland GmbH zulässig.

#### Warenzeichen

NETGEAR® ist ein eingetragenes Warenzeichen von NETGEAR, Inc.

Windows® ist ein eingetragenes Warenzeichen der Microsoft Corporation.

Andere Marken und Produktnamen sind Warenzeichen bzw. eingetragene Warenzeichen ihrer jeweiligen Inhaber. Informationen können ohne Vorankündigung geändert werden.

Alle Rechte vorbehalten

#### Haftungsausschluss

Obwohl bei der Zusammenstellung der in diesem Dokument enthaltenen Informationen größte Sorgfalt angewandt wurde, übernimmt NETGEAR keine Gewähr für deren Korrektheit, Vollständigkeit, Aktualität und Qualität.

Im Interesse, das Design, die Funktionen und die Zuverlässigkeit zu verbessern, behält sich NETGEAR das Recht vor, die in diesem Dokument beschriebenen Produkte oder Verfahren ohne vorherige Ankündigung zu verändern.

NETGEAR übernimmt keine Haftung für den Gebrauch oder Einsatz der Produkte, Schaltungsanordnungen, Anwendungen oder Verfahren, die in diesen Unterlagen beschrieben werden.

In keinem Fall kann NETGEAR für etwaige Schäden ideeller oder materieller Art verantwortlich gemacht werden, die durch die Nutzung oder im Zusammenhang mit der Nutzung der hier bereitgestellten Informationen entstehen, seien es direkte oder indirekte Schäden, Folgeschäden oder Sonderschäden einschließlich entgangenen Gewinns, oder Schäden, die aus dem Verlust von Daten entstehen. Dies gilt selbst dann, wenn ich auf die Möglichkeit solcher Schäden hingewiesen wurde.

**NETGEAR Deutschland GmbH**

Konrad-Zuse-Platz 1 • 81829 München • GERMANY

Tel.: +49 (0)89 / 9 27 93 - 25 00 • Fax: +49 (0)89 / 9 27 93 - 25 10

<http://www.netgear.de>