FAQ FR114W

Die meistgestellten Fragen zum
FR114W xDSL/Kabel ProSafe Wireless-Ready Firewall

1 Was ist ein FR114W xDSL/Kabel ProSafe Wireless-Ready Firewall?

FR114W 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. Es besteht zudem die Möglichkeit, eine NETGEAR IEEE 802.11-basierende 11MBit/s Wireless PCMCIA-Netzwerk-Karte einzustecken. Damit hat man über eine Wireless Access Point Zugriff auf das LAN.

2 Ist es ein Router?

Ja, es ist ein Router und noch viel mehr. Der FR114W stellt alle Funktionalitäten eines NAT (Network Address Translation) Routers bereit und zusätzlich noch viele Sicherheitsfunktionen.

3 Welche besonderen Merkmale hat der FR114W?

Der FR114W sorgt für zusätzliche Sicherheit im Netzwerk, da er vier zusätzliche wichtige Leistungsmerkmale bereitstellt, die in einem konventionellen NAT-Router nicht existieren:

- Statische Content (-Inhalt) Filterung (URL, URL Schlüsselwörter)
- Abweisung von DoS (– Denial of Sevice), Vorbeugung durch genaue Datenpaket-Kontrolle
- Logging, Reporting und Alarm-Meldungen (Intrusion Detection System)

4 Was ist der Unterschied zwischen der FR114W Wireless-Ready Firewall und anderen NAT-Routern?

Der FR114W hat neue Leistungsmerkmale, mit welchen er eine bessere Performance und ein besseres Preis-Leistungsverhältnis erreicht.

Die Spezifikationen des FR114W sind:

- Bessere Firewall-Funktionalitäten
- Einen Schnelleren Prozessor (75Mhz) und einen 10/100-WAN-Port für schnelleren Datendurchsatz und mehr Sicherheit.
- Ein verbessertes Benutzer-Interface für einen schnelleren Netzwerkzugriff und bessere Performance

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

- Remote Management Funktionalitäten für eine einfache Einsatz in Mehreren Standorten.
- Die Upgrade-Möglichkeit zu einem Wireless-Netzwerk. Dies geschieht über eine zusätzliche Wireless-Karte.

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

6 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 genützt 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 benützt. 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.

7 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.

8 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.

9 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 benützt, 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 FR114P ist eine echte Firewall wie andere Produkte aus der ProSafe-Serie. Dies gilt für den FVS318, den FM114P und den FR114P.

10 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 benützt 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.

11 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 Zielserver 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).

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

Der Router prüft jedes Datenpaket und falls er bemerkt, das 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 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.

13 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

14 Was für andere Sicherheitsfunktionen bekommen ich mit dem FR114W?

Zusätzlich zu den echten Firewall Funktionen benützt der FR114W eine 40/64 und eine 128-Bit WEP-Verschlüsselung. Dies schützt das Netzwerk sowohl innerhalb wie auch außerhalb des LANs. Der FR114W wird mit folgender Software ausgeliefert: Fredom Anti-Virus und Privacy Software von Zero Knockledge 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.

15 Wie viele Wireless-Benutzer können vom FR114W unterstützt werden?

Bis zu 32 Benutzer werden unterstützt.

16 Können im FR114W andere Wireless-Karten verwendet werden?

Nein, andere Karten werden vom FR114W nicht unterstützt.

17 Welchen Operations-Radius hat ein Wireless Access Point?

Der Operations-Radius beträgt bis ca. 50 Meter, dieser hängt aber von den Umgebungsbedingungen ab.

18 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.

19 Filtert der FR114W die Inhalte nach diesem Prinzip?

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

20 Wie viele Benutzer werden vom FR114W unterstützt?

Der FR114W kann bis zu 253 Benutzer unterstützen.

21 Wo kann ich das Produkt kaufen?

Bezugsadressen für die FR114W xDSL/Kabel ProSafe Wireless-Ready Firewall finden Sie auf der Web-Seite www.NETGEAR.de.

22 Welcher Prozessor wird im FR114W verwendet?

Der FR114W benützt einen 75Mhz Prozessor mit integriertem 4-Port-Switch.

23 Wie viel Speicher besitzt der FR114W?

Der FR114W verfügt über 1MB Flash Memory und 4 MB DRAM Memory auf dem Board.

24 Welche Plattformen werden vom FR114W unterstützt?

Der FR114W arbeitet auf Plattformen, auf denen das TCP/IP Protokoll eingebunden ist (wie z.B. Macintosh, Linux, Unix, etc.) und kann einen Browser benützten (wie Netscape und Windows IE).

25 Kann der FR114W auch mit anderen als NETGEAR Netzwerkprodukten zusammen arbeiten?

Natürlich funktioniert der FR114W auch mit anderen Nicht-NETGEAR Netzwerkprodukten, wenn diese dem Ethernet Standard (802.3) entsprechen.

26 Wie einfach ist es, sich mit dem FR114W ans Internet anzubinden?

Sie können den FR114W 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 FR114W, verbinden Sie Ihre Computer mit den LAN-Ports und dann konfigurieren Sie den FR114W, indem Sie 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.

27 Ich habe bereits eine 10 oder 100 MBit/s Ethernet Karte, ist diese kompatibel mit dem FR114W?

Ja, der FR114W hat einen eingebauten Autosensing Switch, der sowohl 10 wie auch 100 MBit/s unterstützt.

28 Der FR114W hat einen 10/100MBit/s WAN-Port. Was ist besonders wichtig an diesem Merkmal?

Der 10/100 Port gibt die Möglichkeit, den FR114W an einen schnelleren Breitband-Service (schneller als 10MBit/s) anzubinden. Da diese High Speed Services bis jetzt allerdings keine weit verbreitete Verfügbarkeit haben, stellt der FR114W hierfür einen Migrationspfad zur Verfügung. Viele Router am Markt verfügen hierüber noch nicht.

29 Arbeitet der FR114W mit meinem bestehenden xDSL oder Kabel Internet Service zusammen?

Der FR114W 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.

30 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.

31 Wie kann ich mit dem FR114W auf Internet-Spiele und Anwendungen (z.B. Napster, ICQ, AIM, etc.) zugreifen?

Stellen Sie in der Web-Konfigurationsseite den Public Server (Port Forwarding) ein.

32 Erlaubt der FR114W auch einen „DMZ“?

Ja, der FR114W 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.

33 Es ist mir nicht möglich, eine Web Konfigurations-Seite für den FR114W 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 `winipcfg` aus (Windows ME und älter) oder `ipconfig` auf der Windows NT Plattform, um eine dynamische IP-Adresse zuzuweisen. Dann starten Sie denn Browser.

34 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 xDLS-Zugang für ein ans Ethernet angebundenes xDSL-Modem aufzubauen. Es nützt die Vorteile der geteilten Ethernet-Umgebung zugleich mit PPPs vertrautem und sicheren Dial-Acess Benutzermodel.

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.

35 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 angebundenen 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.

36 Ist es dem FR114W möglich, VPN zu unterstützen?

Ja, der FR114W unterstützt VPN passiv durch IPSec, L2TP und PPTP Pass-through. Das bedeutet, dass Sie einen VPN-Tunnel durch die Firewall aufbauen können, wenn Sie dies in Verbindung mit einer VPN Client-Software machen.

37 Kann der FR114W aktiv einen VPN-Tunnel öffnen oder terminieren?

Nein, denn es unterstützt nur Pass-through. Wenn Sie ein Produkt benötigen, das aktiv einen VPN-Tunnel öffnen oder terminieren kann, informieren Sie sich doch bitte über den NETGEAR FVS318, Information zu diesem Produkt finden Sie unter www.NETGEAR.com.

38 Unterstützt der FR114W 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.

39 Unterstützt der FR114W andere Betriebssysteme?

Ja, der FR114W ist kompatibel zu anderen Betriebssystemen, vorausgesetzt dieses System unterstützt auch TCP/IP (wie zum Beispiel Web-Browser).

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

Sie können dies in der FR114W Konfiguration auf der ‚Content Filtering’ Seite einstellen. Bitte lesen Sie das Handbuch, um eine detaillierte Beschreibung für diese Einstellungen zu bekommen.

41 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.

42 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 oder www.sygatetech.com.

43 Was für weitere Produkte benötige ich, wenn ich einen FR114W einsetzen möchte?

Sie benötigen eine Wireless 802.11b-kompatibele Ethernet Karte und eine Highspeed Breitband Internetverbindung (z.B. xDSL oder Kabel).

44 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

45 Wie kann ich mehr über VPN oder Wireless Technologie erfahren?

Besuchen Sie unsere Web-Seite unter www.netgear.com und klicken Sie „Planet VPN“ an oder schauen Sie sich unter „Produkte“ die komplette Familie unserer Wireless-Produkte 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 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