



NETGEAR

HIPAA Compliance

Vertical Market Applications

● What is HIPAA?

The Health Insurance Portability & Accountability Act of 1996 (August 21), Public Law 104-191, which amends the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act. Among other things this includes:

1. Improved efficiency in healthcare delivery by standardizing electronic data interchange, and
2. Protection of confidentiality and security of health data through setting and enforcing standards.

NETGEAR Firewall devices, like the FVM318, FVL328 and FVS318 are designed to help healthcare organizations comply with the HIPAA mandate.



FVM318 ProSafe Wireless VPN Security Firewall with 70 WAN and 32 WLAN VPN Tunnels



FVL328 ProSafe VPN High-Speed Firewall Router with 100 VPN Tunnels



FVS318 ProSafe VPN Firewall Router with 8 VPN Tunnels

Among the features that NETGEAR devices provide to facilitate compliance are the following:

- Access control
- Audit control
- Authorization control
- Data authentication
- Entity authentication
- Communications/network controls
- Implementation features

HIPAA Requirements

Access Control - 142.308(c)(1)(i)

Features required:

- Procedure for emergency access
- At least one of three features must be implemented
 - context-based control
 - user-based control
 - access based control
- Optional use of encryption

Audit Control - 142.308(c)(1)(ii)

Authorization Control - 142.308(c)(1)(iii)

At least one of the following features must be implemented:

- role-based access
- user-based access

Data Authentication - 142.308(c)(1)(iv)

Entity Authentication - 142.308(c)(1)(v)

The following features must be implemented:

- automatic log-off
- unique user identification

At least one of the following must be implemented:

- biometric
- password
- PIN
- telephone callback
- token

Communications or Network Controls - 142.308(d)(1)(i)

The following features must be implemented:

- integrity controls
- message authentication

Communications or Network Controls - 142.308(d)(1)(ii)

At least one of the following must be implemented:

- access controls
- encryption (over open networks)

Implementation Features - 142.308(d)(2)

The following four features must

be implemented:

- alarm
- audit trail
- entity authentication
- event reporting

NETGEAR Solution

NETGEAR products control incoming and outgoing traffic between the Internet and protected network.

NETGEAR products provide support for user-level control through third-party VPN client software.

NETGEAR products have logging and reporting features that show network access of specific IP addresses, and types of hacker attacks that have been stopped by the firewall.

NETGEAR products offer user-based access controls through the use of a password. Only one user can access the management screen at any given time.

NETGEAR products use data authentication algorithms to ensure that the data has not been altered or destroyed in an unauthorized manner when sent through the firewall.

NETGEAR products use a "time-out" function that will log-off the user after a predetermined time of inactivity.

NETGEAR products use an internal user database that can authenticate via user names and passwords.

NETGEAR products use data authentication algorithms to ensure the integrity of data when sent through the firewall.

NETGEAR products use data encryption algorithms to ensure the integrity of data when sent through the firewall and across the Internet.

NETGEAR products have logging and reporting features that show network access of specific IP addresses, and types of hacker attacks that have been stopped by the firewall.

NETGEAR Products

NETGEAR FVM318, FVS318, FVL328

NETGEAR products support many major VPN client software packages including Microsoft®, SafeNer®, and other major companies.

NETGEAR FVM318, FVS318, FVL328

Secure Sockets Layer (SSL) encrypted Web-based management of FVM318, FVS318, FVL328.

NETGEAR FVM318, FVS318, FVL328 support SHA-1 and MD5 encryption algorithms

NETGEAR FVM318, FVS318, FVL328 support SHA-1 and MD5 encryption algorithms.

NETGEAR FVM318, FVS318, FVL328 support SHA-1 and MD5 authentication algorithms.

IPSec-based 3DES (FVM318, FVS318 and FVL328) and AES (FVM318 and FVS318) encryption are supported.

NETGEAR FVM318, FVS318, FVL328

NETGEAR

4500 Great America Parkway
Santa Clara, CA 95054 USA
Phone: 1-888-NETGEAR
E-mail: info@NETGEAR.com
www.NETGEAR.com

©2003 NETGEAR, Inc. NETGEAR®, the Netgear Logo, Auto Uplink, the Gear Guy, and Everybody's connecting are trademarks or registered trademarks of Netgear, Inc. in the United States and/or other countries. Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other brand and product names are trademarks or registered trademarks of their respective holders. Information is subject to change without notice. All rights reserved.