

Norman Virus Control v5

for Firewall-1 Next Generation

Norman Virus Control (NVC) v5 for Firewall-1 Next Generation offers the most comprehensive virus protection for Checkpoint FireWall-1 NG. This latest version takes advantage of Norman's renowned scanning engine and includes the unique Norman SandBox technology, which supplements NVC's ability to detect even known and unknown computer viruses, including trojans and worms.

Key features

- On-access virus scanning of the HTTP (web), FTP (download) and SMTP (email) protocols.
- Norman's SandBox technology to detect both known and unknown computer viruses, including trojans and worms.
- Comprehensive exclude list to increase performance.
- Automatic updates of virus definition files and other product enhancements over the Internet.

Complete list of topics and features

- Real-time scanning
- Norman SandBox
- Exclude list
- Protocols scanned for computer viruses
- Automatic updates of virus definition files

Real-time scanning

Norman Virus Control for F1-NG offers on-access scanning for computer viruses at the company's firewall, thus ensuring the best network perimeter protection against computer viruses available. If a computer virus is detected, the following options are available:

- Clean
 - Remove
 - Warn only
 - Ignore
- Infected files that cannot be cleaned will be moved into a quarantine area.

Norman SandBox

Norman's SandBox technology detects new and unknown computer viruses, including trojans and worms. Today, an email worm can infect tens of thousands of workstations in a matter of seconds. The antivirus vendors are expected to find the cure, update the virus definition files, and distribute these to its customers immediately. The need for speed is paramount. Norman's SandBox is a virtual world where everything is simulated. An emulator provides an environment where possible virus infected executables «run» just as they would do on a real system. When execution stops, the SandBox is analyzed for changes. The SandBox is particularly tuned to find new email-, network- and peer-to-peer worms.

When new malware is detected, the system administrator receives a message through NVC's messaging system listing the vital facts. When this option is selected, scanning time will increase, but it is not likely to affect the performance considerably.

Exclude list

The exclude list is a list of file type extensions. The file extension is meant to tell the operating system what kind of file it is. Normally all types of files are scanned by the virus scanner. When virus scanning is performed on the FireWall-1, the slight delay imposed by the virus scanner on each file passing through the firewall may add up to significantly slowing down the access through the firewall. The users may experience slow Internet access when all files are scanned. To improve the throughput, some file types may be excluded from virus scan, typically files with static content and without executable programs or scripts.

Protocols scanned for computer viruses

The Norman Virus Control for FireWall-1 NG plug-in protects all traffic that comes into the network over the HTTP, SMTP, or FTP. The various protocols can be configured individually, and protocols can be excluded from being scanned if required.



Peace of Mind

Norman is one of the world's leading companies within the field of data security. With products for virus control, spam control, email control, download control, personal firewall, encryption, data recovery, certified data erasure and computer forensics, the company plays an important role in the data industry.

NORMAN®

www.norman.com



System requirements

Automatic updates

- Norman Internet Update (NIU) is an integrated part of NVC and can be configured to regularly check for new and updated files on Norman's product servers. NIU provides complete updating and upgrading of the application software and virus definition files to ensure that the latest version of the software is always installed.

- NIU employs incremental updates of virus definition files to keep the size of the updates as small as possible, thereby reducing download time.

- - Norman Virus Control for FireWall-1 NG running on Windows 2000 SP2, Windows XP SP1 or higher with Check Point™ FireWall-1. NG FP31 or higher.
- - Norman Virus Control for FireWall-1 NG requires that Norman Virus Control v5.7 or higher is installed with Checkpoint FireWall-1 NG FP3 in working condition.
- - Norman Virus Control for FireWall-1 NG is compatible with Check Point Software.
- - FireWall-1 NG Feature Pack 3 or higher or FireWall-1 AI.

Prerequisites

- To take full advantage of the functions in NVC for FireWall-1, a good understanding of Check Point™ FireWall-1 NG FP3 including the Content Vectoring Protocol (CVP) is required. In addition, a basic knowledge of Norman Virus Control v5 is favorable.



22 x "100%" awards



Norman solutions for clients/workstations: Norman Virus Control for Microsoft Windows 95, 98, Me, NT4.0, 2000, XP, OS/2, Linux (On-Demand scanning) | Norman Internet Control for Microsoft Windows 95, 98, Me, NT4.0, 2000, XP | Norman Personal Firewall | Norman Privacy

Norman solutions for servers: Norman Virus Control for Microsoft Windows NT4.0, 2000, 2003, XP | Norman Virus Control Firebreak for Novell Netware 4.11 and later | Norman Virus Control for Linux

Norman solutions for web, gateways and mail servers: Norman Spam Control | Norman Email Control | Norman Download Control | Norman Virus Control Net | Norman Virus Control for Lotus Domino (Win32, OS/2) | Norman Virus Control for Firewall-1 NG | Norman Virus Control for Microsoft Internet Information Server | Norman Virus Control for Microsoft Exchange | Norman Virus Control for MIMESweeper

NORMAN®

www.norman.com